HUMAN RIGHTS WATCH

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments
That Endorsed Online Learning During
the Covid-19 Pandemic

HUMAN RIGHTS WATCH

STUDENTS NOT PRODUCTS

Printed in the United States of America
ISBN: 978-1-62313-983-4
Cover illustration by: © Andrea Devia Nuño, Hero Studios

Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amsterdam, Beirut, Berlin, Brussels, Chicago, Geneva, Goma, Johannesburg, London, Los Angeles, Moscow, Nairobi, New York, Paris, San Francisco, Sydney, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: HRW.org

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

HUMAN RIGHTS WATCH

STUDENTS NOT PRODUCTS

HUMAN RIGHTS WATCH

STUDENTS NOT PRODUCTS

Summary

On school days, 9-year-old Rodin wakes up every morning at 8 a.m. in Istanbul, Turkey. He eats a bowl of chocolate cereal for breakfast; his mother reminds him, as she always does, to brush his teeth afterwards. By 9 a.m., he logs into class and waves hello to his teacher and to his classmates. He hopes that no one can tell that he's a little sleepy, or that he's behind on his homework.

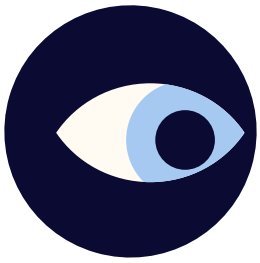
During breaks between classes, Rodin reads chat messages from his classmates and idly doodles on the virtual whiteboard that his teacher leaves open. He watches his best friend draw a cat; he thinks his friend is much better at drawing than he is. Later in the afternoon, Rodin opens up a website to watch the nationally televised math class for that day. At the end of each day, he posts a picture of his homework to his teacher's social media page.

Unbeknownst to him, an invisible swarm of tracking technologies surveil Rodin's online interactions throughout his day. Within milliseconds of Rodin logging into class in the morning, his school's online learning platform begins tracking Rodin's physical location—at home in his family's living room, where he has spent most of his days during the pandemic lockdown. The virtual whiteboard passes along information about his doodling habits to advertising technology (AdTech) and other companies; when Rodin's math class is over, trackers follow him outside of his virtual classroom and to the different apps and sites he visits across the internet. The social media platform Rodin uses to post his homework silently accesses his phone's contact list and downloads personal details about his family and friends. Sophisticated algorithms review this trove of data, enough to piece together an intimate portrait of Rodin in order to figure out how he might be easily influenced.

Neither Rodin nor his mother were aware that this was going on. They were only told by his teacher that he had to use these platforms every day to be marked as attending school during the Covid-19 pandemic.[1]

This report is a global investigation of the education technology (EdTech) endorsed by 49 governments for children's education during the pandemic. Based on technical and policy analysis of 164 EdTech products, Human Rights Watch finds that governments' endorsements of the majority of these online learning platforms put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education.

1 Human Rights Watch interview with Rodin R. and his mother, Istanbul, Turkey, June 11, 2021. The names of all children quoted in this report have been changed to protect their privacy.



Human Rights Watch observed 146 EdTech products directly sending or granting access to children's personal data to 199 AdTech companies.

The coronavirus pandemic upended the lives and learning of children around the world. Most countries pivoted to some form of online learning, replacing physical classrooms with EdTech websites and apps; this helped fill urgent gaps in delivering some form of education to many children.

But in their rush to connect children to virtual classrooms, few governments checked whether the EdTech they were rapidly endorsing or procuring for schools were safe for children. As a result, children whose families were able to afford access to the internet and connected devices, or who made hard sacrifices in order to do so, were exposed to the privacy practices of the EdTech products they were told or required to use during Covid-19 school closures.

Human Rights Watch conducted its technical analysis of the products between March and August 2021, and subsequently verified its findings as detailed in the methodology section. Each analysis essentially took a snapshot of the prevalence and frequency of tracking technologies embedded in each product on a given date in that window. That prevalence and frequency may fluctuate over time based on multiple factors, meaning that an analysis conducted on later dates might observe variations in the behavior of the products.

Of the 164 EdTech products reviewed, 146 (89 percent) appeared to engage in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights. These products monitored or had the capacity to monitor children, in most cases secretly and without the consent of children or their parents, in many cases harvesting data on who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use.

Most online learning platforms installed tracking technologies that trailed children outside of their virtual classrooms and across the internet, over time. Some invisibly tagged and fingerprinted children in ways that were impossible to avoid or get rid of—even if children, their parents, and teachers had been aware and had the desire and digital literacy to do so—without throwing the device away in the trash.

Most online learning platforms sent or granted access to children's data to third-party companies, usually advertising technology (AdTech) companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyze these data to guess at a child's personal characteristics and interests, and to predict what a child might do next and how they might be influenced. Access to these insights could then be sold to anyone—advertisers, data brokers, and others—who sought to target a defined group of people with similar characteristics online.

Children are surveilled at dizzying scale in their online classrooms. Human Rights Watch observed 146 EdTech products directly sending or granting access to children's personal data to 196 third-party companies, overwhelmingly AdTech. Put another way, the number of AdTech companies receiving children's data was discovered to be far greater than the EdTech companies sending this data to them, illustrating the financial incentives that place economic value on children's data and fuel extraordinarily intrusive surveillance and deep erosions of their privacy.

Some EdTech products targeted children with behavioral advertising. By using children's data—extracted from educational settings—to target them with personalized content and advertisements that follow them across the internet, these companies not only distorted children's online experiences, but also risked influencing their opinions and beliefs at a time in their lives when they are at high risk of manipulative interference. Many more EdTech products sent children's data to AdTech companies that specialize in behavioral advertising or whose algorithms determine what children see online.

It is not possible for Human Rights Watch to reach definitive conclusions as to the companies' motivations in engaging in these actions, beyond reporting on what we observed in the data and the companies' and governments' own statements. In response to requests for comment, several EdTech companies denied collecting children's data. Some companies denied that their products were intended for children's use, or stressed that their virtual classroom pages for children's use had adequate privacy protections, even if Human Rights Watch's analysis found that pages adjacent to the virtual classroom pages (such as the login page, home page or adjacent page with children's content) did not. AdTech companies denied knowledge that the data was being sent to them, indicating that in any case it was their clients' responsibility not to send them children's data.

Governments bear the ultimate responsibility for failing to protect children's right to education. With the exception of a single government—Morocco—all governments reviewed in this report endorsed at least one EdTech product that risked or undermined children's rights. Most EdTech products were offered to governments at no direct financial cost to them; in the process of endorsing and ensuring their wide adoption during Covid-19 school closures, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy, access to information, and potentially freedom of thought.

Many governments put at risk or violated children's rights directly. Of the 42 governments that provided online education to children by building and offering their own EdTech products for use during the pandemic, 39 governments produced products that handled children's personal data in ways that risked or infringed on their rights. Some of these governments made it compulsory for students and teachers to use their EdTech product, not only subjecting them to the risks of misuse or exploitation of their data, but also making it impossible for children to protect themselves by opting for alternatives to access their education.

Children, parents, and teachers were denied the knowledge or opportunity to challenge these data surveillance practices. Most EdTech companies did not disclose their surveillance of children through their data; similarly, most governments did not provide notice to students, parents, and teachers when announcing their EdTech endorsements.

In all cases, this data surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most EdTech companies did not allow their students to decline to be tracked; most of this monitoring happened secretly, without the child's knowledge or consent. In most instances, it was impossible for children to opt out of such surveillance and data collection without opting out of compulsory education and giving up on formal learning altogether during the pandemic.

Remedy is urgently needed for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. Governments should conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.

In line with child data protection principles and corporations' human rights responsibilities as outlined in the United Nations Guiding Principles on Business and Human Rights, EdTech and AdTech companies should not collect and process children's data for advertising. Companies should inventory and identify all children's data ingested during the pandemic, and ensure that they do not process, share, or use children's data for purposes unrelated to the provision of children's education. AdTech companies should immediately delete any children's data they received; EdTech companies should work with governments to define clear retention and deletion rules for children's data collected during the pandemic.

As more children spend increasing amounts of their childhood online, their reliance on the connected world and digital services that enable their education will continue long after the end of the pandemic. Governments should develop, refine, and enforce modern child data protection laws and standards, and ensure that children who want to learn are not compelled to give up their other rights in order to do so.

Children should be actively consulted throughout these processes, helping to build safeguards that protect meaningful, safe access to online learning environments that provide the space for children to develop their personalities and their mental and physical abilities to their fullest potential.

Recommendations

To Governments

Facilitate urgent remedy for children whose data were collected during the pandemic and remain at risk of misuse and exploitation. To do so:

- Conduct data privacy audits of the EdTech endorsed for children's learning during the pandemic, remove those that fail these audits, and immediately notify and guide affected schools, teachers, parents, and children to prevent further collection and misuse of children's data.
- Require EdTech companies with failed data privacy audits to identify and immediately delete any children's data collected during the pandemic.
- Require AdTech companies to identify and immediately delete any children's data they received from EdTech companies during the pandemic.
- Prevent the further collection and processing of children's data by technology companies for the purposes of profiling, behavioral advertising, and other uses unrelated to the purpose of providing education.

Adopt child-specific data protection laws that address the significant child rights impacts of the collection, processing, and use of children's personal data. Where child data protection laws already exist, update and strengthen implementation measures to deliver a modern child data protection framework that protects the best interests of the child in complex online environments.

Enact and enforce laws ensuring that companies respect children's rights and are held accountable if they fail to do so. In line with the United Nations Guiding Principles on Business and Human Rights, such laws should require companies to:

- Conduct and publish child rights due diligence processes.
- Provide full transparency in data supply chains, and publicly report on how children's data are collected and processed, where they are sent, to whom, and for what purpose.
- Provide child-friendly, age-appropriate processes for remedy and redress for children who have experienced infringements on their rights; such mechanisms should be transparent, independently accountable, and enforceable.

Require child rights impact assessments in any public procurement processes that provide essential services to children through technology.

Ban behavioral advertising to children. Commercial interests and behavioral advertising should not be considered legitimate grounds of data processing that override a child's best interests or their fundamental rights.

Ban the profiling of children. In exceptional circumstances, governments may lift this restriction when it is in the best interests of the child, and only if appropriate safeguards are provided for by law.

To Ministries and Departments of Education

Where online learning is adopted as a preferred or hybrid mechanism for delivering education, allocate funding to pay for services that safely enable online education, rather than allowing the sale and trading of children's data to finance the services.

Ensure that any services that are endorsed or procured to deliver online education are safe for children. In coordination with data protection authorities and other relevant institutions:

- Require all companies providing educational services to children to identify, prevent, and mitigate negative impacts on children's rights, including across their business relationships and global operations.
- Require child data protection impact assessments of any educational technology provider seeking public investment, procurement, or endorsement.
- Ensure that public and private educational institutions enter into written contracts with EdTech providers that include protections for children's data. Children should not be expected to enter into a contract, and children and guardians cannot give valid consent when it cannot be freely refused without jeopardizing a child's right to education.
- Define and provide special protections for categories of sensitive personal data that should never be collected from children in educational settings, such as precise geolocation data.

Provide child-friendly, age-appropriate, and confidential reporting mechanisms, access to expert help, and provisions for collective action in local languages for children seeking justice and remedy. Such measures should avoid placing undue burden or exclusive responsibility on children or their caregivers to seek remedy from companies by acting individually or exposing themselves in the process.

Develop and promote digital literacy and children's data privacy in curricula. Provide training programs for ministry staff, teachers, and other school staff in digital literacy skills and protection of children's data privacy, to support teachers to conduct online learning for children safely.

Seek out children's views in developing policies that protect the best interests of the child in online educational settings, and meaningfully engage children in enhancing the positive benefits that access to the internet and educational technologies can provide for their education, skills, and opportunities.

To Education Technology Companies

Provide urgent remedy and redress where children's rights have been put at risk or infringed through companies' data practices during the pandemic. To do so:

- Immediately stop collecting and processing children's data for user profiling, behavioral advertising, or any purpose other than what is strictly necessary and relevant for the provision of education.
- Stop sharing children's data for purposes that are unnecessary and disproportionate to the provision of their education. In instances where children's data are disclosed to a third party for a legitimate purpose, in line with child rights principles and data protection laws, enter into explicit contracts with third-party data processors, and apply strict limits to their processing, use, and retention of the data they receive.
- Apply child flags to any data shared with third parties, to ensure that adequate notice is provided to all companies in the technology stack that they are receiving children's personal data, and thus obliged to apply enhanced protections in their processing of this data.
- Inventory and identify children's personal data ingested during the pandemic, and take measures to ensure that these data are no longer processed, shared, retained, or used for commercial or other purposes that are not strictly related to the provision of children's education.
- Companies with EdTech products designed for use by children should stop collecting specific categories of children's data that heighten risks to children's rights, including their precise location data and advertising identifiers.

Undertake child rights due diligence to identify, prevent, and mitigate companies' negative impact on children's rights, including across their business relationships and global operations, and publish the outcomes of this due diligence process.

Respect and promote children's rights in the development, operation, distribution, and marketing of EdTech products and services. Ensure that children's data are collected, processed, used, protected, and deleted in line with child data protection principles and applicable laws.

Provide privacy policies that are written in clear, child-friendly, and age-appropriate language. These should be separate from legal and contractual terms for guardians and educators.

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for rights abuses when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged abuses, and should effectively end ongoing infringements on rights.

To Advertising Technology Companies and other Third-Party Companies that May Receive Data from EdTech Products

Inventory and identify all children's data received through tracking technologies the technology companies own and take measures to promptly delete these data and ensure that these data are not processed, shared, or used. To do so:

- Identify all apps and websites that have installed tracking technologies owned by technology companies and transmitted user data to them.
- Of these, classify and create a list of services primarily directed at children, which should be monitored and updated periodically. Notify the parent companies of these services that they need to provide explicit evidence that their service is not made for children to remove their product from this list.
- Using this list, companies should review and promptly delete any children's data received from services made for children.

Prevent the use of technology companies' tracking technologies to surveil children, or any user of these services designed for use by children.

- Regularly audit incoming data and the companies sending them. Delete or otherwise disable the use of any received children's data or user data received from services designed for use by children, when detected.
- Notify and require companies and clients that use tracking technologies to declare any children's data collected through these tools with a child flag or through other means, so that tagged data can be automatically flagged and deleted before transmission to third-party companies.

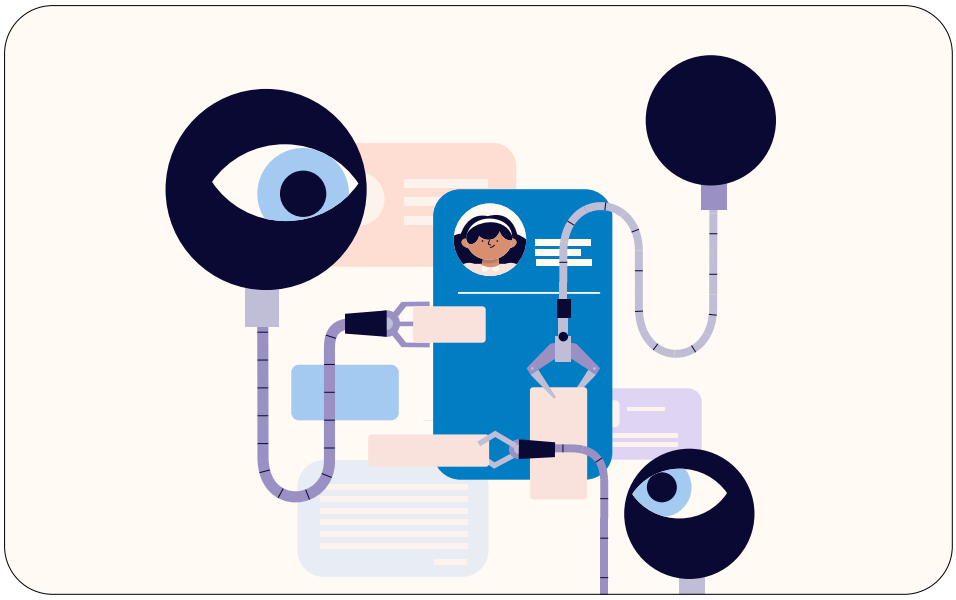
Develop and implement effective processes to detect and prevent the commercial use of children's data collected by technology companies' tracking technologies.

Undertake child rights due diligence to identify, prevent, and mitigate technology companies' impact on children's rights, including across their business relationships and across global operations, and publish the outcomes of this due diligence process..

Provide children and their caregivers with child-friendly mechanisms to report and seek remedy for infringements on rights when they occur. Remedies should involve prompt, consistent, transparent, and impartial investigation of alleged infringements, and should end ongoing violations.

Methodology

This report covers 49 countries that recommended 164 educational technology (EdTech) products for children to use for online learning during Covid-19 school closures.



Human Rights Watch conducted technical analysis on each product to assess how it handled children's data, then compared the results to the product's privacy policy to determine whether the EdTech company disclosed its data practices to children and their caregivers. Human Rights Watch also examined the advertising technology (AdTech) companies and data brokers found to receive children's data, and analyzed the marketing materials and developer documentation of those found to be receiving significant amounts of children's data.

The methods used in this report were free and available for use by governments prior to endorsing or procuring any of the EdTech products analyzed here. While a tool that was used to analyze websites, Blacklight, was published in September 2020, the tests it runs to identify privacy-infringing technologies were individually available and free to use in the form of various privacy census tools built over the past decade. As of November 2021, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.

Human Rights Watch invites experts, journalists, policymakers, and readers to recreate, test, and engage with our findings and research methods. Our datasets, preserved evidence, and a detailed technical methodology can be found online.

Selection Criteria

Human Rights Watch examined the Covid-19 education emergency response plans, documents, and announcements of 68 of the world's most populous countries. Of these, 49 countries adopted online learning as a component of their national plans for continued learning throughout school closures. The EdTech products endorsed or procured by these ministries or departments of education were included for analysis in this report.

In countries where the education ministry recommended a large number of EdTech products—in some cases, numbering in the hundreds—a Mersenne Twister pseudorandom number generator was used to randomly select a maximum of ten products that would serve as an illustrative sample of that education ministry's decisions.[2]

2 Widely used in statistics, computer science, and cryptography, a Mersenne Twister is a pseudorandom number generator, or an algorithm that generates a sequence of numbers that are fairly random. See: Wikipedia, "Mersenne Twister," https://en.wikipedia.org/wiki/Mersenne_Twister (accessed November 8, 2021).

Seven countries—Australia, Brazil, Canada, Germany, India, Spain, and the United States—delegate significant decision-making authority to state—or regional—level education authorities. During the pandemic, this included decisions about what EdTech to endorse or procure for school use. Human Rights Watch identified the two most populous states or provinces in these countries and included their EdTech endorsements for analysis. Similarly for the United Kingdom, the two most populous constituent countries—England and Scotland—were identified for analysis.

As a result, 164 products were analyzed from the following 49 countries: Argentina, Australia (New South Wales, Victoria), Brazil (Minas Gerais, São Paulo), Burkina Faso, Cameroon, Canada (Quebec)[3], Chile, China, Colombia, Côte d'Ivoire, Ecuador, Egypt, France, Germany (Baden-Württemberg, Bavaria), Ghana, Guatemala, India (Maharashtra, national, Uttar Pradesh), Indonesia, Iran, Iraq, Italy, Japan, Kazakhstan, Kenya, Malawi, Malaysia, Mexico, Morocco, Nepal, Nigeria, Pakistan, Peru, Poland, Republic of Korea, Romania, Russian Federation, Saudi Arabia, South Africa, Spain (Andalucía, Catalonia), Sri Lanka, Taiwan, Thailand, Turkey, United Kingdom (England, Scotland), United States (California, Texas), Uzbekistan, Venezuela, Vietnam, and Zambia.

Product Types

Of the 164 EdTech products investigated by Human Rights Watch, 39 were mobile applications ("apps"), 91 were websites, and 34 were available in both formats. Of the products available in both app and website formats, Human Rights Watch analyzed both, except for four products where the app versions were no longer available online, or offered only in iOS, Apple's operating system.

Apps running on Google's Android operating system are the focus of this report. Android is the dominant mobile operating system worldwide, in large part due to the ubiquity of lower-cost mobile phones that run Android.[4] Children living in the countries covered by this report are more likely to have access to an Android device, if they have access to a device at all. This was reflected in the choices that governments made: almost all EdTech products endorsed by the governments covered in this report offer their apps for the Android platform.

In addition, Android's open architecture makes it possible to easily access and observe the interactions between an app and the operating system, as well as to identify the data transmissions from the device running the app to online servers.

While this report focuses on apps built for Android, apps built for Apple's iOS can also employ data tracking technologies and target behavioral advertising to users.[5]

3 Canada's Ontario, and the single EdTech product that it recommended, was originally included in our analysis. After additional rounds of data verification and analysis of the EdTech product, which yielded an inconclusive assessment, Human Rights Watch removed Ontario from its list.

4 By one estimate, Android has 72.83 percent market share worldwide, with iOS taking up 26.35 percent. See: StatCounter, "Mobile Operating System Market Share Worldwide, June 2020-June 2021," https://web.archive.org/web/20210728054452/https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed July 27, 2021).

5 Thorin Klosowski, "We Checked 250 iPhone Apps–This is How They're Tracking You," New York Times, May 6, 2021, https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/ (accessed April 14, 2022); Thorin Klosowki, "Looking Back on a Year of Apple's Privacy Labels and Tracking," New York Times, March 31, 2022, https://www.nytimes.com/wirecutter/blog/apple-privacy-labels-tracking/ (accessed April 14, 2022).

Access and Archival

To investigate how EdTech products handled children's data and their rights, Human Rights Watch downloaded a copy of the latest version of the product and its privacy policy between February 19 and March 15, 2021. Human Rights Watch conducted the primary phase of its investigation between March and August 2021, and conducted further checks in November 2021 to verify findings.

To preserve documentation and to invite readers to recreate, test, and engage with our findings, the privacy policy, and EdTech website or app were archived, whenever available, on the Internet Archive's Wayback Machine. The versions of the EdTech apps examined by Human Rights Watch are listed in the appendices.

EdTech products were sorted into the following categories:

1. Products that do not require a user account to access learning content;
2. Products that offer the choice to sign up for an optional user account;
3. Products that require a user account to access learning content; and
4. Products that require verification of the child's identity as a student, either by their school or their ministry of education, to set up a mandatory account to access the service.

To avoid misleading EdTech companies as to our affiliation and the nature of our research, no user accounts were created for products identified in categories 1, 2, and 4.

Human Rights Watch created user accounts for a limited number of EdTech products in category 3. As it is possible to disassemble and analyze apps' code without having to sign into a user account, accounts were created only for 27 websites in this category to test for privacy violations in the same environment used by children to attend classes. In these instances, Human Rights Watch explicitly identified the nature of our engagement, populating mandatory input fields with the following values to signal our affiliation and intent. Optional fields were left blank.

Email: iamaresearcher@hrw.org
User name: hrwresearcher
Organization / School name: Human Rights Watch
First Name: HRW
Last Name: Researcher
Phone number: [a real number]

Throughout its investigation, Human Rights Watch did not interact with other users or enter into virtual classrooms.

Human Rights Watch did not create user accounts for products in category 4, as that would have entailed falsely assuming the identity of a real student. For these websites, technical analysis was restricted to webpages that children likely had to interact with in order to access their virtual classroom, prior to logging in, such as the product's home page or login page.

Some of the companies that offered EdTech products in category 4 told Human Rights Watch that the virtual classrooms and related spaces accessible to children after the login were adequately protective of privacy. These companies asserted that the pages before their product's login (e.g., the login page, home page, or adjacent page designed for children) were designed for use by teachers, parents and other adults, and not properly described as designed for children's use.

Technical Analysis: Apps

There are two methods of disassembling and analyzing a mobile app. The first is through static analysis, which analyzes an app's code and identifies its capabilities, or the functions and instructions that may be executed when the app is run. The second is through dynamic analysis, which runs the app under realistic conditions and observes what data is transmitted where, and to whom.

Human Rights Watch conducted manual static analysis tests on 73 apps, using Android Developer Studio to decompile the app and to analyze its code. All results were verified by scanning each app using Pithus, an open source mobile threat intelligence platform that conducts automated static analysis tests on mobile apps, and εxodus by εxodus Privacy, an open source privacy auditing platform that scans for trackers embedded in Android apps, and corroborating the results against Human Rights Watch's analyses.[6]

Additionally, Human Rights Watch commissioned Esther Onfroy, founder of Defensive Lab Agency, and the creator of both Pithus and εxodus Privacy, to conduct in-depth static and dynamic analysis on eight apps, which were used as a final check to ensure the accuracy of our results.

Dynamic Analysis and Children's Participation

Human Rights Watch collaborated with four children from India, Indonesia, South Africa, and Turkey who participated in an in-depth investigation to uncover how an EdTech app recommended by their government handled their privacy.

These children and their guardians were informed of the nature and purpose of our research, that they would receive no personal service or benefit for speaking to us, and our intention to publish a report with the information gathered. Human Rights Watch requested and received consent from the children and their guardians, and informed each that they were under no obligation to speak with us or to participate in the project.

Human Rights Watch asked each child to download a virtual private network (VPN) and the EdTech app on their mobile device. They were then asked to open, run, and close the VPN and the EdTech app several times within a single day, interacting with the app as if they were using it for school or for learning. After 24 hours, children deleted both from their phones.

Esther Onfroy of the Defensive Lab Agency received the data files and analyzed them to identify data flows and transmissions. These findings were corroborated against dynamic analysis conducted on each app, using a VPN to simulate app usage in the child's country. This methodology design maximally protected children's privacy by encrypting the child's data and ensuring that only the data flows could be analyzed, without revealing the substance of children's personal data.

All children's data were securely stored, then deleted, at the end of the investigation. The data files for one child's experiment were provided to the child, at their request.

6 Pithus, "Mobile threat intelligence for the masses," https://beta.pithus.org/ (accessed September 21, 2021); εxodus Privacy, "Exodus Privacy," https://exodus-privacy.eu.org/en/ (accessed September 21, 2021).

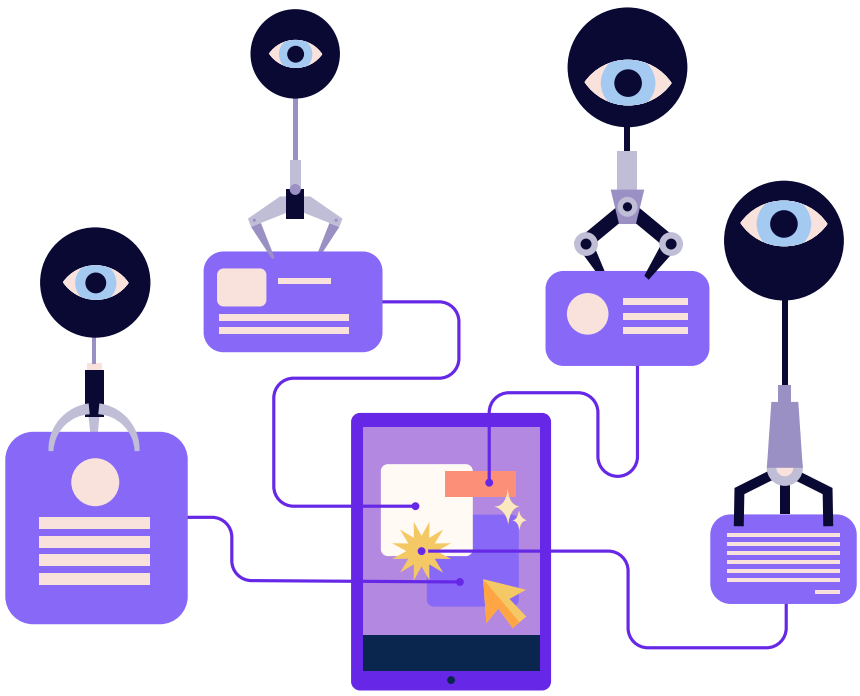
Technical Analysis: Websites

To understand how websites handle children's data, Human Rights Watch used Blacklight, a real-time website privacy inspector built by Surya Mattu, senior data engineer and investigative data journalist at The Markup.[7]

Released in September 2020, Blacklight emulates how a user might be surveilled while browsing the web.[8] The tool scans any website, runs tests for seven known types of surveillance, and returns an instant privacy analysis of the inspected site. Built on the foundation of robust privacy census tools built over the past decade, Blacklight monitors scripts and network requests to observe when and how user data is being collected, and records when this data is being sent to known third-party AdTech companies.[9]

Blacklight exists in two formats: as a user-friendly interface on The Markup's website, and as an open source command-line tool.[10] Human Rights Watch chose to work with the latter, as it provides the flexibility to adapt the tool to provide customized analysis, as well as a higher observational power that yields fine-grained evidence of the surveillance it detects on websites. Surya Mattu of The Markup generously assisted Human Rights Watch in customizing Blacklight for this investigation.

In order to recreate the experience of a child using an EdTech website in their country, and how their data might be collected, handled, and sent to third parties, Human Rights Watch conducted all technical tests while running a VPN set to the country where the product was endorsed by the government for children's education. This proved essential: early tests conducted by Human Rights Watch found that the prevalence of surveillance technologies embedded in a website changed depending on the country the website believed that its user was located. Many of the observed differences appeared to be related to that country's data protection laws, where they exist.



7 The Markup, "Blacklight," https://themarkup.org/blacklight (accessed September 21, 2021).

8 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 7, 2021).

9 Ibid. AdTech companies and their domains were identified by using DuckDuckGo Tracker Radar. See: DuckDuckGo, "DuckDuckGo Tracker Radar Exposes Hidden Tracking," March 5, 2020, https://spreadprivacy.com/duckduckgo-tracker-radar/ (accessed March 1, 2021).

10 The Markup, "Blacklight Collector," GitHub, https://github.com/the-markup/blacklight-collector (accessed March 1, 2021); The Markup, "Blacklight Reporter," GitHub, https://github.com/the-markup/blacklight-reporter (accessed March 1, 2021).

Human Rights Watch selected for examination websites that were explicitly recommended by governments for use for children's online education. In response to Human Rights Watch's findings, some companies noted that their government-recommended products were designed for use by teachers, parents and other adults, and not for use by children. Accepting those claims as fact, this still raises the question of why the governments recommended pages for use by children that were not adequately vetted to protect their privacy, as well as the question of whether the companies should have changed their privacy practices on those pages once the government made its recommendation.

Technical Limitations

Analyzing apps using static analysis may yield false positives, as not all of the app's source code might be implemented in practice when a user runs the app. Put another way, an app may not use all of the programmed functionalities of which it is capable. Human Rights Watch notes this limitation by distinguishing between analysis of the code's capabilities (static analysis) and detections of actual transmission of children's data (dynamic analysis) throughout the report.

A technical analysis does not definitively determine the intent of any particular tracking technology, or how the collected data is used. For example, an EdTech product can include third party computer code that collects information that may be useful to monitor the product's performance and stability. The same data collected by the same third-party code may also be used in tandem with other third-party code to enable data collection for advertising or other marketing purposes. In a static analysis, it is not possible to conclude whether user data were collected, or the scope or purpose of the data collection. Neither is it possible solely with a technical analysis to determine how the collected data is used by the third party.

As another example, third-party computer code embedded in a product to perform an administrative function can be designed also to enable access to a device's camera, microphone, or another feature. In a static analysis, it is possible to detect the capability, but not whether the capability is utilized. In addition, the EdTech company implementing such third-party code for an administrative function may not have plans to enable those features, and may not be aware of the possibility. Note also that access by any code to an Android device's camera or microphone is possible only if the user settings on the device enable such sharing.

Where possible, Human Rights Watch worked to reduce ambiguity by examining the parent companies that own the tracking technologies found in an EdTech product, as well as the companies found to receive transmissions of children's data. Human Rights Watch conducted further analysis on companies that receive, analyze, trade, or sell people's personal data for commercial and other purposes, and reviewed their publicly available marketing materials and developer documentation.

Blacklight's analysis is limited by three other factors: the simulation may trigger different surveillance responses from the website under examination, because it is a simulation of user behavior, not actual user behavior; the possibility of producing false positives while scanning for canvas fingerprinting; the possibility of producing false negatives through a stack tracing technique. Further investigation by The Markup determined that the probability of these false errors occurring is very low, and that Human Rights Watch's methodology design may have further reduced this risk.[11] A detailed discussion of these technical limitations can be found on Blacklight's methodology, available online.[12]

11 According to The Markup, false positives with canvas fingerprinting occur "very occasionally" when Blacklight is run in the cloud, because it is difficult to distinguish the tool from any other bot. As Human Rights Watch conducted its technical tests by running Blacklight on a local machine with a VPN, this, in theory, would have further reduced the risk of false positives. Furthermore, The Markup notes that the stack tracing technique did not produce false negatives in their tests or in their survey of the 100,000 most popular websites on the internet. See: Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," The Markup, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 7, 2021).

12 Ibid.

For readers seeking to replicate Human Rights Watch's findings, it is important to note that the observed behavior of these apps and websites, and the detected prevalence and frequency of tracking technologies embedded in them, may fluctuate. This is influenced by multiple factors, including the geographical location of the user, date and time of testing, and the device or browser type, among other variables. In addition, apps and websites that use AdTech services to offer advertisers and other third-party companies the opportunity to target their students with ads through an electronic high-frequency trading process known as real-time bidding, further described in Chapter 1, may yield different results as to the recipient of the children's data, as different third parties may have won the bid each time.

Human Rights Watch conducted manual analysis on four websites—Distance Learning (Cameroon), Eduyun (China), Smart Revision (Zambia), and e-learning portal (Zambia)—on which Blacklight tests failed for a variety of technical failures. One site was incompatible with the browser used by Blacklight, and another refused to load upon detecting the VPN service used by Human Rights Watch. The manual analysis conducted on these four sites followed the same methodology used by the Blacklight tool.

Interviews with Children, Parents, and Teachers

Human Rights Watch interviewed students, parents, and teachers between April 2020 and April 2021 about their experiences with online learning. Interviewees were based in the following 17 countries: Australia, Chile, Denmark, Germany, Indonesia, India, Iran, Italy, Lebanon, Republic of Korea, Russia, Serbia, Spain, South Africa, Turkey, United Kingdom, and the United States.

Interviewees lived in capital cities, other cities, Indigenous communities, rural and remote locations, suburbs, towns, and villages.

Interviews were conducted directly, or with interpretation, in Arabic, Bahasa Indonesian, Danish, English, Ewe, Farsi, German, Hindi, Italian, Korean, Russian, Serbian, Spanish, and Turkish.

Interviewees were not paid to participate. Interviewees were informed of the purpose of the interview, its voluntary nature, and the ways in which the information would be used. They provided oral and written consent to be interviewed.

Many parents and teachers requested that their names not be used in this report to protect their privacy or the privacy of their children or students, or to feel free to speak about their school, or for cultural reasons. Children's identities are protected with pseudonyms of their own choosing. Pseudonyms are reflected in the text with a first name followed by an initial and are noted in the footnotes.

Requests for Comment

Human Rights Watch shared the findings presented in this report with 95 EdTech companies, 199 AdTech companies, and the 49 governments covered in this report, and gave them the opportunity to respond and provide comments and clarifications. Of these, 48 EdTech companies, 78 AdTech companies, and 10 governments responded as of May 24, 2022 at 12:00pm EDT.

I. Covid-19, Education, and Technology

There were no doubts that the online platforms and tools used could be unsafe. It was never questioned.

— A single mother of two school-aged boys, Izhevsk, Udmurt Republic, Russia11[13]

Covid-19 and Children's Education

The novel coronavirus has devastated children's education around the world.[14] On March 11, 2020, the World Health Organization (WHO) declared that an outbreak of Covid-19 had reached global pandemic levels. Within weeks, almost every country in the world closed down their schools in an attempt to stop the spread of Covid-19, upending the lives and learning of 1.6 billion children and young adults, or 90 percent of the world's students.[15] By March 2021, a full year into the pandemic, half of the global student population remained shut out of school.[16]

Most countries pivoted to some form of online learning, replacing physical classrooms with phones, tablets, and computers.[17] This deepened existing inequities in children's access to education, in the form of digital divides between children with access to technologies critical for online learning, and those without. It also created a dependence and need for affordable, reliable connectivity and devices so overwhelming that it triggered global shortages for both. Supply chains for computers buckled under staggering demand, as shortages of essential parts created two-year shipment delays

13 Human Rights Watch interview with mother, Izhevsk, Russia, June 12, 2020.

14 Human Rights Watch, "*Years Don't Wait for Them": Increased Inequalities in Children's Right to Education Due to the Covid-19 Pandemic* (New York: Human Rights Watch, 2021), https://www.hrw.org/report/2021/05/17/years-dont-wait-them/increased-inequalities-childrens-right-education-due-covid.

15 United Nations Educational, Scientific and Cultural Organization (UNESCO) Institute for Statistics, "Education: From disruption to recovery," 2021, https://en.unesco.org/covid19/educationresponse/ (accessed June 21, 2021).

16 UNESCO, "One Year into Covid-19 Education Disruption: Where Do We Stand?" March 19, 2021, https://en.unesco.org/news/one-year-covid-19-education-disruption-where-do-we-stand (accessed June 21, 2021).

17 Online learning was the most used remote learning method by governments worldwide. According to a survey of 129 countries, 90 percent offered learning through online platforms. UNESCO, UNICEF, World Bank, "What Have We Learnt? Overview of Findings from a Survey of Ministries of Education on National Responses to Covid-19," October 2020, https://data.unicef.org/resources/national-education-responses-to-covid19/ (accessed June 22, 2021), p. 21.

worldwide and pitted desperate schools and education ministries against one another.[18] As more people became heavily reliant on the internet to work, communicate, play, and study during Covid-19 lockdowns, the resulting explosion of traffic clogged the internet and dumped unprecedented stress on its infrastructure. Nine days after the WHO's pandemic declaration, the European Commission took the extraordinary step of asking internet companies, video streaming services, and gaming platforms to reduce their services in Europe to reserve bandwidth for work and education.[19]

Teachers and schools faced a bewildering array of digital platforms to choose from as they scrambled to set up virtual classrooms. In response, governments issued endorsements of educational technologies (EdTech) for use. Some governments rapidly signed contracts with EdTech companies to purchase millions of licenses for teachers and students.[20]

As a result, EdTech companies experienced explosive, unprecedented demand for their products. In the days and weeks after the WHO's pandemic declaration, education app downloads worldwide surged 90 percent compared to the weekly average at the end of 2019.[21] Children spent significantly more time online in virtual classrooms; by September 2020, the number of hours spent in education apps globally each week had increased to an estimated 100 million hours, up 90 percent compared to the same period in 2019.[22]

Google Classroom, Google's teacher-student communication platform, reported that the pandemic had almost quadrupled its users to more than 150 million, up from 40 million in 2019; similarly, G Suite for Education, Google's classroom software, reported doubling its users to more than 170 million students and educators.[23] "We have seen incredible growth," Javier Soltero, a vice president at the company, said in an interview with *Bloomberg*. "It actually mirrors, unfortunately, the ramp up and spread of the disease."[24]

The explosive demand also generated record revenues and profits. As the global economy plummeted, venture capital financing for EdTech startups surged to a record-setting US$16.1 billion in 2020, more than doubling the $7 billion raised in 2019.[25] Two companies, Byju's and Yuanfudao, became the first EdTech companies to achieve "decacorn" status—an exclusive group of the world's most valuable privately-held

18 Kellen Browning, "The Digital Divide Starts With a Laptop Shortage," *New York Times*, October 12, 2020, https://www.nytimes.com/2020/10/12/technology/laptops-schools-digital-divide.html (accessed June 22, 2021); Paresh Dave, "Laptops, desktop sales see 'renaissance'; shortages won't ease until 2022," *Reuters*, December 24, 2020, https://www.reuters.com/article/us-tech-hardware-yearend/laptops-desktop-sales-see-renaissance-shortages-wont-ease-until-2022-idUSKBN28Y12M (accessed June 22, 2021).

19 Hadas Gold, "Netflix and YouTubeare slowing down in Europe to keep the internet from breaking," *CNN Business*, March 20, 2020, https://www.cnn.com/2020/03/19/tech/netflix-internet-overload-eu/index.html (accessed June 21, 2021); Klint Finley, "YouTube Slashes Video Quality to Save Bandwidth," *WIRED*, March 24, 2020, https://www.wired.com/story/youtube-slashes-video-quality-save-bandwidth/ (accessed June 21, 2021); Cecilia Kang, Davey Alba, and Adam Satariano, "Surging Traffic is Slowing Down Our Internet," *New York Times*, March 26, 2020, https:/www.nytimes.com/2020/03/26business/coronavirus-internet-traffic-speed.html (accessed June 21, 2021).

20 See, for example, Microsoft Stories Asia, "Enabling A Digital Future for Vietnam," Microsoft, July 8, 2020, https://web.archive.org/web/20210819180052/https://news.microsoft.com/apac/2020/07/08/enabling-a-digital-future-for-vietnam/ (accessed July 28, 2021); Microsoft News Center, "Egypt's Ministry of Education Makes Office 365 Available For All Students And Teachers Through New Online Self-Services Portal," Microsoft, December 21, 2020, https://web.archive.org/web/20210819180141/https://news.microsoft.com/en-xm/2020/12/21/the-ministry-of-education-signs-an-agreement-with-microsoft-to-provide-a-unified-platform-for-students-and-teachers/ (accessed July 28, 2021); Mitch Tarica, "Zoom Selected by Los Angeles Unified School District," post to "Zoom Blog" (blog), Zoom, July 2, 2020, https://web.archive.org/web/20210819175013/https://blog.zoom.us/zoom-selected-by-los-angeles-unified-school-district/ (accessed August 19, 2021); Board of Education of the City of Los Angeles, "Regular Meeting Order of Business," June 8, 2021, https://web.archive.org/web/20210819175920/http://laschoolboard.org/sites/default/files/06-08-21RegBdOBMaterialsWithLinksPublic.pdf (accessed August 19, 2021), p. 29.

21 Lexi Sydow, "Mobile Minute: Global Classrooms Rely on Education Apps As Remote LearningAccelerates," post to "App Annie" (blog), App Annie, April 8, 2020, http://web.archive.org/web/20200416093942/https://www.appannie.com/en/insights/mobile-minute/education-apps-grow-remote-learning-coronavirus/ (accessed June 22, 2021).

22 Lexi Sydow, "Mobile Minute: Remote Return to School Sees 90% Boost Across Top Education Apps," post to "App Annie" (blog), App Annie, September 23, 2020, http://web.archive.org/web/20200926051917/https://www.appannie.com/en/insights/mobile-minute/top-education-apps-growth-2020/ (accessed June 22, 2021).

23 In February 2021, Google rebranded G Suite for Education to Google Workspace for Education Fundamentals. See: Melanie Lazare, "A Peek At What's Next for Google Classroom," post to Google: The Keyword (blog), February 17, 2021, https://web.archive.org/web/20210819180239/https://blog.google/outreach-initiatives/education/classroom-roadmap/ (accessed June 21, 2021); Shantanu Sinha, "More Options for Learning With Google Workspace for Education," post to Google: The Keyword (blog), February 17, 2021, https://web.archive.org/web/20210819180354/https://www.blog.google/outreach-initiatives/education/google-workspace-for-education/ (accessed June 21, 2021).

24 Gerrit De Vynck and Mark Bergen, "Google Classroom Users Doubled as Quarantines Spread," Bloomberg Quint, April 9, 2020, https://www.bloomberg.com/news/articles/2020-04-09/google-widens-lead-in-education-market-as-students-rush-online (accessed June 21, 2021).

25 HolonIQ, "Global EdTech Venture Capital Update – Q1 2021," March 31, 2021, http://web.archive.org web/20220104184935/https://www.holoniq.com/notes/global-edtech-venture-capital-update-q1-2021/ (accessed June 22, 2021).

companies, valued at more than $10 billion—after attracting millions of new students and closing successful financing rounds during the pandemic.[26]

Technology companies that provided free services to schools also benefited, gaining significant market share as millions of students became familiar with their product. Zoom Video Communications, which provided free services to more than 125,000 schools in 25 countries, as well as limited free services for the general public, reported its sales skyrocketing 326 percent to $2.7 billion and its profits propelled from $21.7 million in 2019 to $671.5 million in 2020.[27]

The use of EdTech helped governments to fill urgent gaps and deliver some measure of learning during the pandemic. However, governments' endorsements and procurements of EdTech also turbocharged the mass collection of children's data, exposing their personal information to the risk of misuse and exploitation by the advertising-driven internet economy and resulting in the mass surveillance of children's lives, both inside and outside of the classroom.

How the Internet-Based Economy Works

We don't monetize the things we create. We monetize users.

—Andy Rubin, creator of Android, the world's most widely used mobile operating system[28]

Today's internet is powered by the advertising technology (AdTech) industry. Motivated by the belief that personalized ads are more persuasive and therefore more lucrative, AdTech companies collect massive troves of data about people to target them with ads tailored to their presumed interests and desires. The revenue generated by digital advertising pays for most of the services available on the internet today.

26 Anu Raghunathan, "Indian EdTech Billionaire's Byju's Becomes Decacorn After Funding Round from Mary Meeker," Forbes, June 29, 2020, https://www.forbes.com/sites/anuraghunathan/2020/06/29/indian-edtech-billionaires-byjus-becomes-decacorn-after-funding-round-from-mary-meeker/ (accessed June 22, 2021); Priyamvada Mathur, "China's Yuanfudao Claims Global EdTech Valuation Crown," Pitchbook, October 22, 2020, https://pitchbook.com/news/articles/yuanfudao-edtech-valuation-china (accessed June 22, 2021).

27 Zoom, "Teaching, Learning & Connecting in 2020: Education in an Extraordinary Year," post to "Zoom Blog" (blog), Zoom, December 21, 2020, https://web.archive.org/web/20210819180503/https://blog.zoom.us/connecting-in-2020-education-in-an-extraordinary-year/ (accessed July 28, 2021); Zoom, "Annual Report, Fiscal 2021," https://web.archive.org/web/20210819180624/https://investors.zoom.us/static-files/a17fd391-13ae-429b-8cb3-bfd95b61b007 (accessed July 28, 2021); Zoom, "Zoom Video Communications Reports Fourth Quarter and Fiscal Year 2021 Financial Results," March 1, 2021, https://web.archive.org/web/20210819180506/https://investors.zoom.us/news-releases/news-release-details/zoom-video-communications-reports-fourth-quarter-and-fiscal-o (accessed July 28, 2021).

28 Steven Levy, "The Inside Story of the Moto X: The Reason Google Bought Motorola," *WIRED*, August 1, 2013, https://www.wired.com/2013/08/inside-story-of-moto-x/ (accessed June 21, 2021).

Most internet companies offer their website, app, or content for free, or charge a negligible fee that does not reflect the full cost of offering these services. Instead of asking people to pay for these services with money, companies require people to give up their data and attention, often without their knowledge or meaningful consent.[29] Companies then traffic their users' data into a complex ecosystem of AdTech companies, data brokers, and others in a set of highly profitable transactions that make up a $378.16 billion industry.[30]

Here's how a child using an EdTech app to attend her school online might interact with the AdTech industry. This illustration similarly describes a child's experience using an EdTech website to attend her school online.

1. EdTech companies that make educational apps for children decide to send a child's personal data to third-party companies and possibly to sell ads in their apps, in order to generate revenue.

2. AdTech companies help put ads in apps. They make packages of code, such as software development kits (SDKs) and other tracking technologies, for app makers to insert into their apps to personalize and display ads to their users. When this code is installed in the app, this code collects data that may be used by the AdTech company to target advertising, whether on the EdTech product or on another site or app.

3. A child opens the EdTech app that their school uses for online learning and logs in for class.

4. Instantly, the app begins to collect personal data about the child. This can include who the child is, where she is, what she does, who she interacts with in her virtual classroom, and what kind of device her parents can afford for her to use.

5. This data can be sent to AdTech companies, either by the EdTech app, or directly by the AdTech SDKs embedded in the app. In the process, AdTech companies assign an ID number to the child, so that they can piece together the data they receive to build a profile on her.

6. Some AdTech companies will also follow the child across the internet and over time. Some may search for even more information about her from public and private sources, adding definition and detail to an intimate profile of the child.

7. AdTech companies' sophisticated algorithms analyze the trove of data received from the app. They guess at the child's personal characteristics and interests (for example, that she's likely to be female), and predict her future behavior (this child is likely to buy a toy).

8. AdTech companies use these insights to sell to advertisers the ability to target ads to people. This happens through real-time bidding platforms, where algorithms engage in a high-frequency auction amongst advertisers to sell off the chance to show an ad to a user—in this case, a child—to the highest bidder. From start to finish, the automated process of buying and selling between advertisers takes less than a hundred milliseconds and takes place tens of billions of times each day.31

29 Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads (*New York: Knopf, 2016).

30 Several data protection authorities have recognized the economic value of users' data and companies' economic incentives to collect them, in addition to the rights associated with the collection and use of personal data. In addition, some digital platforms have explicitly acknowledged the link between the 'free' nature of their services and their use of advertising. See: Australian Competition and Consumer Commission, "Digital Platforms Inquiry, Preliminary Report," December 10, 2018, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry.pdf (accessed July 9, 2021) pp. 166-167; Ethan Cramer-Flood, "Worldwide Digital Ad Spending 2021," *Insider Intelligence / eMarketer*, April 29, 2021, https://www.emarketer.com/content/worldwide-digital-ad-spending-2021 (accessed June 23, 2021).

31 See: Mike Downey, "Real-Time Bidding Is The Next Mobile Ad Breakthrough – Here's How You Can Profit," *VentureBeat*, July 23, 2012, https://venturebeat.com/2012/07/23/real-time-bidding-is-the-next-mobile-ad-breakthrough-heres-how-you-can-profit/ (accessed June 23, 2021); Jun Wang, Weinan Zhang, and Shuai Yuan, "Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting," June 18, 2017, https://arxiv.org/pdf/1610.03013.pdf (accessed June 23, 2021); Amazon Web Services, "Real-Time Bidding for Advertising & Marketing," http://web.archive.org/web/20210623132624/https://aws.amazon.com/advertising-marketing/adtech-real-time-bidding/ (accessed June 23, 2021); Tim Hwang, Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet (New York: Farrar, Straus and Giroux, 2020), p. 20.

9. These insights can also be sold or shared with data brokers, law enforcement and governments, or others who wish to target a defined group of people with similar characteristics online.

A handful of the world's most valuable internet companies own entire AdTech supply chains. Alibaba, Amazon, Facebook (Meta),32 Google, Microsoft, Tencent, and Yandex offer digital services that serve as the primary channels that most of the world relies on to engage with the internet.33 In turn, they collect extensive data about the billions of people who use or interact with these platforms. They analyze this data to infer and create new information about people, then commercialize those insights for advertising—often on their own real-time bidding platforms.

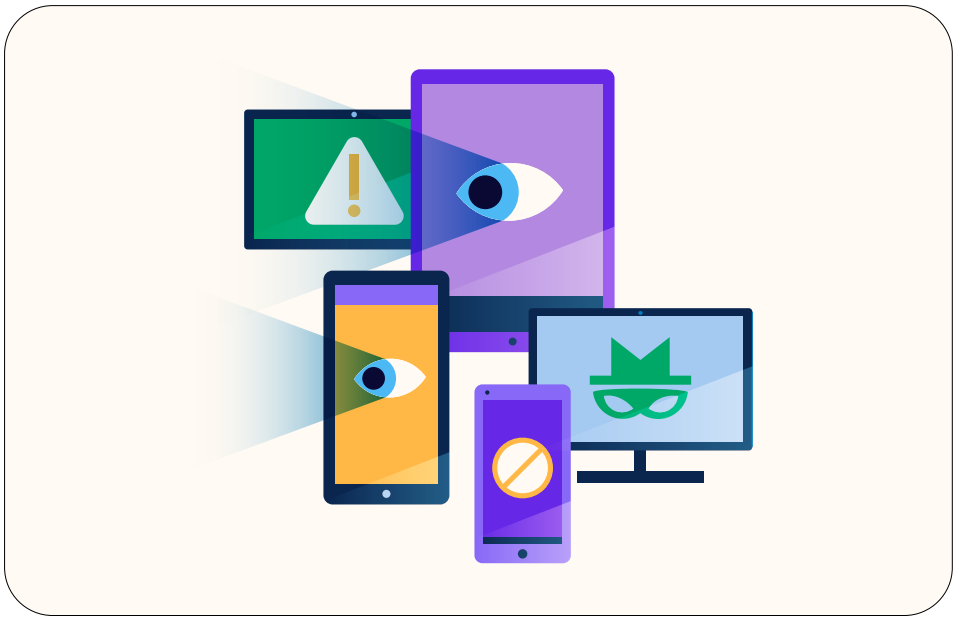
These AdTech companies may also draw upon their vast troves of data to build and offer finely-tuned tracking technologies, prediction models, and microtargeting tools to help advertisers reach their audiences. As further described in Chapter 3, these tools are embedded in most websites and apps that people use every day, enabling these AdTech companies to collect and receive data not just from people directly using their services, but from anyone who encounters their data tracking embedded across the internet. The unparalleled power of these dominant tech companies to collect, track, and combine data across much of the internet results in a powerful and pervasive surveillance of people's lives that is extremely difficult to avoid.[34]

32 Facebook rebranded itself to Meta in October 2021. This report refers to Facebook as both the platform and the parent company, for consistency across the timeline of this investigation.

33 See: Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/ (accessed May 5, 2021); Ethan Cramer-Flood, "Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl," *eMarketer*, May 10, 2021, https://www.emarketer.com/content/duopoly-still-rules-global-digital-ad-market-alibaba-amazon-on-prowl (accessed May 12, 2021); Fortune, "Global 500," 2021, https://fortune.com/global500/ (accessed December 10, 2021).

34 United States Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, "Investigation of Competition in Digital Markets," 2020, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf (accessed September 1, 2021), pp. 51-57; "Bundeskartellamt prohibits Facebook from combining user data from different sources," Bundeskartellamt press release, February 7, 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3591568 (accessed September 1, 2021); "Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector," European Commission press release, June 22, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143 (accessed September 1, 2021); Kashmir Hill, "I Tried to Live Without the Tech Giants. It Was Impossible." *New York Times*, July 31, 2020, https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html (accessed July 29, 2021).

II. Hidden Surveillance: Children's Data Harvested



How dare they? How dare [these companies] peep into my private life?

—Rodin R., 9-year-old student, Istanbul, Turkey[35]

Children's Data and their Right to Privacy

Privacy is a human right.[36] Recognized under international and regional human rights treaties, this right encompasses three connected components: the freedom from intrusion into our private lives, the right to control information about ourselves, and the right to a space in which we can freely express our identities.[37]

Privacy is about autonomy and control over one's life. It is the ability to define for ourselves who we are to the world, on our own terms. This is especially important for children, who are entitled to special protections that guard their privacy and the space for them to grow, play, and learn.[38]

35 Human Rights Watch interview with Rodin R., 9, Istanbul, Turkey, June 25, 2021. The names of all children quoted in this report have been changed to protect their privacy.

36 International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, art. 17; Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, art. 16; Convention on the Rights of Persons with Disabilities, adopted December 13, 2006, G.A. Res. 61/106, Annex I, UN GAOR, 61st Sess., Supp. (No. 49) at 65, UN Doc. A/61/49 (2006), entered into force May 3, 2008, art. 22; African Charter on the Rights and Welfare of the Child, OAU Doc. CAB/LEG/24.9/49 (1990), entered into force November 29, 1999, art. 10; American Convention on Human Rights ("Pact of San José, Costa Rica"), adopted November 22, 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123, entered into force July 18, 1978, , reprinted in Basic Documents Pertaining to Human Rights in the Inter-American System, OEA/Ser.L.V/II.82 doc.6 rev.1 at 25 (1992), art. 11; Council of Europe, European Convention on Human Rights, adopted November 4, 1950, entered into force September 3, 1953, art. 8; Universal Declaration of Human Rights (UDHR), adopted December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), art. 12.

37 Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/ (accessed May 5, 2021), p. 19, UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 5; UN Human Rights Committee, *Coeriel and Aurik v. the Netherlands*, December 9, 1994, Communication No. 453/1991, para. 10.02.

38 In his 2021 report to the UN Human Rights Council, the Special Rapporteur on the right to privacy stated that children's right to privacy "enables their access to their other rights critical to developing personality and personhood, such as the rights to freedom of expression and of association and the right to health, among others." See: UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, paras. 67-76.

Children's privacy is vital to ensuring their safety, agency, and dignity.[39] At school, privacy enables the very purpose of education by providing the space for children to develop their personalities and abilities to their fullest potential.[40] For children who are survivors of abuse, privacy might mean the freedom to live safely, without exposing where they live, play, and go to school.[41] For lesbian, gay, bisexual and transgender (LGBT) children, privacy could mean the difference between seeking life-saving information and being sent to jail, or worse.[42]

As children spend increasing amounts of their lives online, international human rights bodies have recognized that even the mere generation, collection, and processing of a child's personal data can threaten their privacy, because in the process they lose control over information that could put their privacy at risk.[43] Data about children's identities, activities, communications, emotions, health, and relationships merit special consideration, as the handling of such data may result in arbitrary or unlawful abuses of children's privacy and in harms that may continue to affect them later in life.[44]

The United Nations Committee on the Rights of the Child has emphasized that any digital surveillance of children, together with any associated automated processing of their data, should not be conducted routinely, indiscriminately, or without the child's knowledge or, in the case of very young children, that of their parent or caregiver.[45] Moreover, it should not take place "without the right to object to such surveillance, in commercial settings and educational and care settings," and "consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose."[46] Any restriction upon a child's privacy is only permissible if it meets the standards of legality, necessity, and proportionality.[47]

The unprecedented, mass use of education technologies (EdTech) by schools during the pandemic without adequate privacy protections drastically compromised children's right to privacy. Recognizing this, the UN special rapporteur on the right to privacy warned that, "Schools and educational processes need not and should not undermine the enjoyment of privacy and other rights, wherever or however education occurs."[48]

39 Ibid.; Committee on the Rights of the Child, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 67; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 11.

40 CRC, General Comment No. 1, (2001), Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001). For more on children's privacy rights in schools, see: Human Rights Watch, *Leave No Girl Behind in Africa: Discrimination in Education against Pregnant Girls and Adolescent Mothers* (New York: Human Rights Watch, June 2018), https://www.hrw.org/report/2018/06/14/leave-no-girl-behind-africa/discrimination-education-against-pregnant-girls-and#6484; "*I Had a Dream to Finish School": Barriers to Secondary Education in Tanzania* (New York: Human Rights Watch, February 2017), https://www.hrw.org/report/2017/02/14/i-had-dream-finish-school/barriers-secondary-education-tanzania#7406; "*Like Walking Through a Hailstorm": Discrimination against LGBT Youth in US Schools* (New York: Human Rights Watch, December 2016), https://www.hrw.org/report/2016/12/08/walking-through-hailstorm/discrimination-against-lgbt-youth-us-schools; "Submission by Human Rights Watch to the UN Special Rapporteur on the Right to Privacy," October 19, 2020, https://www.hrw.org/news/2020/10/19/submission-human-rights-watch-un-special-rapporteur-right-privacy; Hye Jung Han, "Singapore Spying on Students' Laptops," commentary, Human Rights Dispatch, February 5, 2021, https://www.hrw.org/news/2021/02/05/singapore-spying-students-laptops; "Facial Recognition Technology in US Schools Threatens Rights," commentary, Human Rights Dispatch, June 21, 2019, https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights.

41 Human Rights Watch, "*My Life is Not Your Porn": Digital Sex Crimes in South Korea* (New York: Human Rights Watch, June 16, 2021), https://www.hrw.org/report/2021/06/16/my-life-not-your-porn/digital-sex-crimes-south-korea.

42 Human Rights Watch, *No Support: Russia's "Gay Propaganda" Law Imperils LGBT Youth* (New York: Human Rights Watch, December 11, 2018), https://www.hrw.org/report/2018/12/11/no-support/russias-gay-propaganda-law-imperils-lgbt-youth.

43 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 67-68; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 7; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, June 30, 2014, para. 20; UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, para. 71.

44 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 68.

45 Ibid., para. 75.

46 Ibid.

47 UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, June 30, 2014, para. 23; UN Human Rights Council, "Resolution adopted by the Human Rights Council on 23 March 2017," Resolution 34/7, A/HRC/RES/34/7, para. 2; CRC, General Comment No. 1, (2001), Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001).

48 UN Human Rights Council, Report of the Special Rapporteur on the right to privacy on artificial intelligence and privacy, and children's privacy, A/HRC/46/37, January 25, 2021, https://undocs.org/A/HRC/46/37 (accessed August 3, 2021), para. 110.

As described below, many EdTech products endorsed by governments and used by children to continue learning during Covid-19 school closures were found to harvest children's data unnecessarily and disproportionately, for purposes unrelated to their education. Worse still, this data collection took place in virtual classrooms and educational settings online, without giving children the ability to object to such surveillance.[49] In most instances, it was impossible for children to opt out of such data collection without opting out of compulsory schooling and giving up on learning altogether during the pandemic.

Finding Out Who Children Are

To figure out who people are on the internet, advertising technology (AdTech) companies tag each person with a string of numbers and letters that acts as an identifier number that is persistent and unique: it points to a single child or their device, and it does not change.[50]

While the tools described in this discussion are ascribed to AdTech companies, the same tools can be used by other companies, including EdTech companies, to collect data about how their users (including children) use the product. Information about how a user or customer interacts with the product is useful, for example, for the company to improve its product and user experience. In our discussion in this section, we focus our discussion to AdTech companies to simplify the discussion, but the same concepts apply to technology companies that are not in AdTech.

Persistent identifiers enable AdTech companies to infer the interests and characteristics of individual children. Every time a child connects to the internet and comes into contact with tracking technology, any information collected about that child—where they live, who their friends are, what kind of device their family can afford for them—is tied back to the identifier associated with them by that AdTech company, resulting in a comprehensive profile over time. Data tied together in this way do not need a real name to be able to target a real child or person.

In addition, computers can correctly re-identify virtually any person from an anonymized dataset, using just a few random pieces of anonymous information.[51] Given the risks of re-identification, many existing data protection laws recognize persistent identifiers as personal information, granting them the same considerations and legal protections.[52]

Some persistent identifiers are built solely to be used for advertising. Other identifiers identify and track people across multiple devices, across the internet, or trail them from the online world into the physical world. And some identifiers are so inescapably tenacious that they are impossible to avoid or get rid of, without throwing one's device away in the trash.

49 Ibid.

50 Bennett Cyphers and Gennie Gebhart, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance," Electronic Frontier Foundation, 2019, https://www.eff.org/wp/behind-the-one-way-mirror (accessed July 12, 2021).

51 Computer scientists have proven that personal information cannot be protected by current methods of 'anonymizing' data. Advertisers, data brokers, and others have long shared and sold people's personal information without violating privacy laws, under the claim that they anonymize this data by stripping people's real names out. However, computer algorithms can correctly re-identify, for example, 99.98 percent of people from almost any anonymized data set with just 15 data points, such as gender, ZIP code, or marital status. Similarly, knowing just four random pieces of information from an anonymized dataset is enough to re-identify shoppers as unique individuals and uncover the rest of their credit card records, or to uniquely identify people from four locations they were previously at. See: Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," Nature Communications, vol. 10 (2019), accessed June 30, 2021, doi: 10.1038/s41467-019-10933-3; Yves-Alexandre de Montjoye et al., "Unique in the shopping mall: On the reidentifiability of credit card metadata," Science, vol. 347, no. 6221 (2015), accessed June 30, 2021, doi:10.1126/science.1256297, pp. 536-539; Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," Nature Scientific Reports vol. 3 (2013), accessed June 30, 2021, doi:10.1038/srep01376.

52 See, for example, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016/679, Official Journal of the European Union, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed July 29, 2021), para. 30; Ibid., art. 4 (1), L 119/33; US Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," July 2020, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (accessed July 29, 2021), art. A (3).

Apps: Persistent Identifiers

Advertising Identifiers

Of the 73 EdTech apps examined by Human Rights Watch, 41 apps (56 percent) were found collecting their users' advertising IDs. This allowed these apps to tag children and identify their devices for the sole purpose of advertising to them.

An advertising ID is a persistent identifier that exists for a single use: to enable advertisers to track a person, over time and across different apps installed on their device, for advertising purposes. For those using an Android device, this is called the Android Advertising ID (AAID). An AAID is neither necessary nor relevant for an app to function; Google's developer guidelines stipulate that app developers must "only use an Advertising ID for user profiling or ads use cases."[53]

The 41 apps that were found to have the capability to collect AAID were endorsed by 29 governments for children's learning during Covid-19. Altogether, these apps identify, tag, and track an estimated 6.24 billion users, including children.

Of these, 33 apps appear to have the ability to collect AAID from an estimated 86.9 million children, because their own materials describe and appear to market them for children's education, with children apparently intended as their primary users.

App	Country	Apparently designed for use by children?	Developer	Estimated Users[54]
Minecraft: Education Edition	Australia: Victoria	Yes	Private	500,000
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, United States: California	No	Private	1,000,000
Descomplica	Brazil: São Paulo	Yes	Private	1,000,000
Stoodi	Brazil: São Paulo	Yes	Private	1,000,000
Storyline Online	Canada: Quebec	Yes	Private	50,000
Remind	Colombia	Yes	Private	10,000,000
Dropbox	Colombia	No	Private	1,000,000,000
Edmodo	Colombia, Egypt, Ghana, Nigeria, Romania, Thailand	Yes	Private	10,000,000
Padlet	Colombia, Germany: Bavaria, Romania	No	Private	5,000,000
SchoolFox	Germany: Bavaria	Yes	Private	100,000
itslearning	Germany: Bavaria	Yes	Private	1,000,000
Ghana Library App	Ghana	No	Government	10,000

53 Android for Developers, "Best Practices for Unique Identifiers," July 1, 2021, https://web.archive.org/web/20210706170748/https://developer.android.com/training/articles/user-data-ids (accessed July 6, 2021).

54 As verified by Google Play Store user installs globally, as of October 2021.

Diksha	India: Maharashtra, National, Uttar Pradesh)	Yes	Government	10,000,000
e-Pathshala	India: Maharashtra, National, Uttar Pradesh)	Yes	Government	1,000,000
Rumah Belajar	Indonesia	Yes	Government	1,000,000
Quipper	Indonesia	Yes	Private	1,000,000
Ruangguru	Indonesia	Yes	Private	10,000,000
Kelas Pintar	Indonesia	Yes	Private	1,000,000
Shad	Iran	Yes	Government	18,000,000[55]
Newton	Iraq	Yes	Government	50,000
WeSchool	Italy	Yes	Private	1,000,000
schoolTakt	Japan	Yes	Private	1,000
Study Sapuri	Japan	Yes	Private	500,000
Bilimland	Kazakhstan	Yes	Private	500,000
Daryn Online	Kazakhstan	Yes	Private	1,000,000
Kundelik	Kazakhstan	Yes	Private	1,000,000
Muse	Pakistan	Yes	Private	10,000
Taleemabad	Pakistan	Yes	Private	1,000,000
Naver Band	Republic of Korea	No	Private	50,000,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Miro	Romania	No	Private	1,000,000
Kinderpedia	Romania	Yes	Private	10,000
My Achievements	Russian Federation	Yes	Government	100
iEN	Saudi Arabia	Yes	Government	500,000
Extramarks	South Africa	Yes	Private	100,000
Nenasa	Sri Lanka	Yes	Government	50,000
PaGamO	Taiwan	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000
Eğitim Bilişim Ağı	Turkey	Yes	Government	10,000,000
Özelim Eğitimdeyim	Turkey	Yes	Government	500,000
Schoology	US: Texas	Yes	Private	5,000,000

55 Shad is a learning app that is built and offered by the Iranian Ministry of Education for children's learning during Covid-19 school closures. It is not offered through the Google Play Store; no externally verified source for user downloads exist for this app, though the government has self-reported 18 million installs of Shad as of October 28, 2021. See: Government of Iran, Ministry of Education, "Shad," https://web.archive.org/web/20211028212342/http://www.shad.ir/ (accessed October 28, 2021).

None of these apps allowed their users to decline to be tracked. In fact, this data collection is invisible to the child, who simply sees the app's interface on their device. This activity is even more covert in 27 apps that fail to inform their students—either through their privacy policy, or elsewhere on their product—that the app and its embedded third-party AdTech trackers may collect their device's AAIDs in order to track, profile, and target students with advertising. In doing so, these apps deny children, parents, and teachers knowledge of this practice and the ability to consent, and impede their right to effective remedy (as discussed in Chapter 4).[56]

Collectively, these EdTech apps may have provided 33 AdTech companies with access to their students' AAIDs. This was done through software development kits (SDKs), or packages of code embedded in an EdTech app that can be used to facilitate the transmission of users' personal data to advertisers.

Notably, nine governments—Ghana, India, Indonesia, Iran, Iraq, Russia, Saudi Arabia, Sri Lanka, and Turkey—directly built and offered eleven learning apps that may collect AAID from children. In doing so, these governments granted themselves the ability to track an estimated 41.1 million students and teachers purely for advertising and monetization.

Some governments disclosed in their app's privacy policy that the app collects students' AAID for commercial purposes. Rumah Belajar, for example, is an EdTech website and app developed and operated by Indonesia's Ministry of Education and Culture to provide online education to preschool, primary, and secondary school students during the pandemic.[57] Through Rumah Belajar's privacy policy, the Indonesian government discloses that it automatically collects children's "unique device identifiers" and "mobile device unique ID," which may be used to "show advertisements to you," "to advertise on third party websites to you after you visited our service," and shared with third party "business partners" so that they can "offer you certain products, services or promotions."[58]

Through dynamic analysis commissioned by Human Rights Watch and conducted by the Defensive Lab Agency, Human Rights Watch detected students' AAID sent from Rumah Belajar to Google and to Facebook. Specifically, children's AAID were sent to the Google-owned domain **app-measurement.com**, and to the Facebook-owned domain **graph.facebook.com**.[59]

Indonesia does not have a data protection law, or specific regulations that protect children's data privacy. A draft data protection bill, introduced in January 2020 and pending further discussion in the House of Representatives as of September 2021, does not provide dedicated protections for children.[60]

In contrast, Eğitim Bilişim Ağı, developed by Turkey's Ministry of National Education for preschool, primary, and secondary school students to continue learning during Covid-19 school closures, does not provide a privacy policy at all. Nor does the app provide a disclosure elsewhere on the product to notify students that their AAID is collected and sent to third-party companies for advertising purposes.[61]

Through dynamic analysis, Human Rights Watch detected students' AAID transmitted from Eğitim Bilişim Ağı to Google via the Google-owned domains **www.googleadservices.com** and **app-measurement.com. www.googleadservices.com** is operated by Google Ads, the company's online advertising platform. Google Ads uses the information it collects to

56 Android offers users the ability to manually reset the AAID, which would, in theory, make it more difficult for advertisers to associate a child's activities with the digital dossier compiled on their past behaviors. In reality, most users, particularly children, are unlikely to be aware of this, or go to the trouble to find and manually reset their AAID. Furthermore, the ability to reset the AAID is only effective if it is the only persistent identifier collected and transmitted; if the AAID is collected alongside other identifiers, the tracker can not only continue to track the same child, but they can also determine that the AAID had been reset.

57 Kementerian Pendidikan dan Kebudayaan, "Kemendikbud Gandeng Swasta Siapkan Sistem Belajar Daring," March 15, 2020, https://www.kemdikbud.go.id/main/blog/2020/03/kemendikbud-gandeng-swasta-siapkan-sistem-belajar-daring (accessed July 6, 2021).

58 Rumah Belajar, "Privacy Policy," February 4, 2020, http://apps.belajar.kemdikbud.go.id/privacypolicy.html (accessed July 6, 2021).

59 For further discussion on these findings, please refer to the SDK section later in this chapter.

60 While children's data are categorized as "personal data of a specific nature," the draft data protection bill makes no mention of the significance of this definition. Nor does it provide any specific protections to data of this nature. See: Dewan Perwakilan Rakyat Republik Indonesia, "DPR Officially Extends Discussion on PDP Bill and Disaster Management" ("DPR Resmi Perpanjang Pembahasan RUU PDP dan Penanggulangan Bencana"), June 22, 2021, https://www.dpr.go.id/berita/detail/id/33528 (accessed July 29, 2021); Personal Data Protection Bill ("RUU tentang Perlindungan Data Pribadi"), https://web.kominfo.go.id/sites/default/files/users/4752/Rancangan%20UU%20PDP%20Final%20%28Setneg%20061219%29.pdf (accessed July 29, 2021), art. 3(3)(g).

61 The Google Play Store requires app developers to post a link to the app's privacy policy. Instead of pointing to a privacy policy, Eğitim Bilişim Ağı's privacy policy link points back to the home page of its website, https://www.eba.gov.tr/, which also does not have a privacy policy. See: "EBA," Google Play Store, https://web.archive.org/web/20210526213628/https://play.google.com/store/apps/details?id=tr.gov.eba.hesap (accessed July 6, 2021).

understand a person's interests and auctions off to the highest bidder the chance to show an ad to those in the advertiser's target audience.[62]

Neither Indonesia's Ministry of Education and Culture nor Turkey's Ministry of National Education responded to Human Rights Watch's requests for comment. Cisco informed Human Rights Watch that Webex does not collect AAIDs.

The collection of AAID from children is neither necessary nor proportionate to the purpose of providing them with education, and risks exposing children to rights abuses as discussed in Chapter 3.

Inescapable Surveillance

Human Rights Watch found 14 EdTech apps with access to either the Wi-Fi Media Access Control (MAC) address or the International Mobile Equipment Identity (IMEI) on children's devices, two persistent identifiers that are so strong that a child or their parent cannot avoid or protect against their surveillance even if they take the extraordinary step of wiping their phones or performing a factory reset.

Eight apps granted themselves the ability to collect the Wi-Fi MAC address of a device's networking hardware. Located in any device that can connect to the internet, this identifier is extremely persistent and cannot be changed by wiping the device clean with a factory reset. Any instance of an app collecting the Wi-Fi MAC address is notable; in 2015, Google banned developers from accessing the Wi-Fi MAC address over privacy concerns that it was being used by third-party tracking companies as a persistent identifier that could not realistically be changed by users.[63]

Recommended by 13 governments, these apps had the ability to collect the Wi-Fi MAC addresses of an estimated 15.6 billion users. Three of these apps appear to have the ability to do so from an estimated 610,000 children, as their own materials describe and appear to market them for children's education.

App	Country	Apparently designed for use by children?	Developer	Estimated Users[64]
Minecraft: Education Edition	Australia: Victoria	Yes	Private	500,000
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Private	10,000,000,000
Padlet	Colombia, Germany: Bavaria, Romania	No	Private	5,000,000
LINE	Japan, Taiwan	No	Private	500,000,000
Muse	Pakistan	Yes	Private	10,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Extramarks	South Africa	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000

62 See, for example, Google Ads, "Display Campaigns," https://web.archive.org/web/20210825072918/https://ads.google.com/intl/en_us/home/campaigns/display-ads/ (accessed August 25, 2021); Google Ads, "Discovery Ads," https://web.archive.org/web/20210825072911/https://ads.google.com/intl/en_us/home/campaigns/discovery-ads/ (accessed August 25, 2021).

63 In research commissioned by the Australian Competition and Consumer Commission, security researchers from AppCensus noted security vulnerabilities in Android that, when exploited, allow apps to collect the Wi-Fi MAC by circumventing the permission systems' protections. See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_0.pdf (accessed April 3, 2021), pp. 17, 47. See also: Android for Developers, "Android 6.0 Changes," March 11, 2021, https://developer.android.com/about/versions/marshmallow/android-6.0-changes (accessed July 7, 2021).

64 As verified by Google Play Store user installs, as of October 2021.

Nine apps were found with the ability to collect International Mobile Equipment Identity (IMEI) numbers. Used to connect to cellular networks and to trace stolen phones, every mobile device has an IMEI number baked into its hardware. An IMEI cannot be changed, and it is illegal to do so in some countries.[65] The only means of changing one's IMEI is to throw the phone away and purchase a new one.

Recommended for children's learning by 12 governments, these apps may have collected in the aggregate IMEI numbers from an estimated 6.6 billion users. Four of these apps are apparently designed exclusively for children, so they may collect IMEI numbers from an estimated 3.1 million children in Brazil, Indonesia, Pakistan, and South Africa.

App	Country	Apparently designed for use by children?	Developer	Estimated Users[66]
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Private	1,000,000
Stoodi	Brazil: São Paulo	Yes	Private	1,000,000
Kelas Pintar	Indonesia	Yes	Private	1,000,000
LINE	Japan, Taiwan	No	Private	500,000,000
Taleemabad	Pakistan	Yes	Private	1,000,000
Telegram	Russia	No	Private	1,000,000,000
KakaoTalk	Republic of Korea	No	Private	100,000,000
Extramarks	South Africa	Yes	Private	100,000
Facebook	Taiwan	No	Private	5,000,000,000

Human Rights Watch found 10 apps potentially engaging in ID bridging. When the AAID is collected and bundled alongside another persistent device identifier, the resulting "bridge" between the two is so powerful that it bypasses any privacy controls that the user may have set on their device to protect themselves. This allows companies to track users with an AAID that can never be reset, in effect creating an accurate advertising profile of a user that lasts in perpetuity.[67]

65 For example, see: Mobile Phones (Re-programming) Act 2002, UK Public General Acts, 2002 c.31, Section 1, https://www.legislation.gov.uk/ukpga/2002/31/section/1 (accessed July 7, 2021); Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017, Government of India Ministry of Telecommunications, August 25, 2017, https://dot.gov.in/sites/default/files/2017_10_23%20Prevention%20of%20Mobile%20Tempering.pdf (accessed July 7, 2021).

66 As verified by Google Play Store user installs globally, as of October 2021.

67 International Digital Accountability Council, "Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic," September 1, 2020, https://digitalwatchdog.org/privacy-considerations-as-schools-and-parents-expand-utilization-of-ed-tech-apps-during-the-covid-19-pandemic/ (accessed December 10, 2020), pp. 11-12.

Given the risks that ID bridging poses to users' privacy, Google's own policies warn developers that the "advertising identifier may not be connected to persistent device identifiers (for example: SSAID, MAC address, IMEI, etc.) for any advertising purpose."[68]

App	Country	Apparently designed for use by children?	Potential ID bridging	Developer	Estimated Users[69]
Minecraft: Education Edition	Australia: Victoria	Yes	Wi-Fi MAC	Private	500,000
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	IMEI	Private	1,000,000
Stoodi	Brazil: São Paulo	Yes	IMEI	Private	1,000,000
Padlet	Germany: Bavaria, Romania, Colombia	Yes	Wi-Fi MAC	Private	1,000,000
Kelas Pintar	Indonesia	Yes	IMEI	Private	1,000,000
Muse	Pakistan	Yes	Wi-Fi MAC	Private	10,000
Taleemabad	Pakistan	Yes	IMEI	Private	500,000
KakaoTalk	Republic of Korea	No	Wi-Fi MAC, IMEI	Private	100,000,000
Extramarks	South Africa	Yes	Wi-Fi MAC, IMEI	Private	100,000
Facebook	Taiwan	No	Wi-Fi MAC, IMEI	Private	5,000,000,000

Muse, for example, was conclusively found to be engaging in ID bridging. Through dynamic analysis, Human Rights Watch observed Muse collecting and transmitting bridged ID data to Facebook through the Facebook-owned domain **graph.facebook.com**.

Of the 14 apps discovered to grant themselves access to their users' Wi-Fi MAC or IMEI, 10 did not disclose this in their privacy policies. None of the 10 apps found to engage in ID bridging disclosed this practice to their users.

When reached for comment, Cisco informed Human Rights Watch that Webex neither collects IMEI information nor engages in ID bridging. Microsoft denied that Minecraft: Education Edition engages in ID bridging, and Padlet responded that it did not intend to collect the data needed for ID bridging. In their responses, Facebook (Meta) and Muse did not answer whether their products engage in ID bridging. Kakao declined to respond to our request for comment; Extramarks, Kelas Pintar, Stoodi, and Taleemabad did not respond.[70]

These practices are not necessary for EdTech apps to function or for the purpose of providing children's education.

68 Google Play Console, "Ads," https://web.archive.org/web/20210707220131/https://support.google.com/googleplay/android-developer/answer/9857753 (accessed July 7, 2021).

69 As verified by Google Play Store user installs globally, as of October 2021.

70 Human Rights Watch email correspondence with Robyn Blum, Global Corporate Communications, Cisco, January 19, 2022; with Steve Crown, Vice President and Deputy General Counsel, Microsoft, April 15, 2022; with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; with Hassan Bin Rizwan, Founder, SABAQ / MUSE, April 2, 2022; and with Suwon Kim, Policy Team, Kakao Corp., April 21, 2022.

Websites: Canvas Fingerprinting

Of the many tracking technologies that websites can use to identify people and their behaviors online, one of the most invasive is canvas fingerprinting. Virtually impossible for users to block, this technique works by drawing hidden shapes and text on a user's webpage. Because each computer draws these shapes slightly differently, these images can be used by marketers and others to assign a unique number to a user's device, which is then used as a singular identifier to track the user's activities across the internet.[71] Users cannot protect themselves by using standard web browser privacy settings or ad-blocking software.

Of the 125 EdTech websites examined by Human Rights Watch, eight websites were found "fingerprinting" their users and tracking them across the internet.

Notably, two of these websites are directly built and operated by government—Moscow Electronic School (Russia) and Digital Lessons (Russia)—for children's educational use. Another website, CBC Kids (Canada), receives the majority of its funding from government.[72]

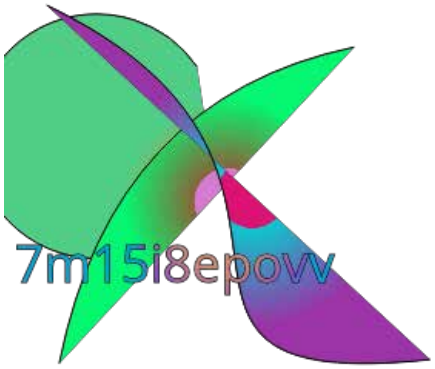
Website	Country	Apparently designed for use by children?	Developer	Canvas fingerprinting script loaded from:
CBC Kids	Canada: Quebec	Yes	Government	https://gem.cbc.ca/akam/11/4c588f3 https://www.cbc.ca/akam/11/b62e49a
WorkFlowy	Colombia	No	Private	https://workflowy.com/media/js/82cab8d21714ada491b4.js https://workflowy.com/media/js/auth_embed.min.js
Top Parent	India: Uttar Pradesh	Yes	Private	https://cdnjs.cloudflare.com/ajax/libs/fingerprintjs2/2.1.0/fingerprint2.min.js
WeSchool	Italy	Yes	Private	https://m.stripe.network/out-4.5.35.js
Z-kai	Japan	Yes	Private	https://spider.af/t/k5lcn2yw?s=01&o=-9vd5xkmg7be&a=1623564108947&u= https://spider.af/t/k5lcn2yw?s=01&
iMektep	Kazakhstan	Yes	Private	https://st.vk.com/js/cmodules/mobile
Moscow Electronic School	Russia	Yes	Government	https://stats.mos.ru/ss2.min.js
Digital Lessons	Russia	Yes	Government	https://st.vk.com/js/cmodules/mobile

One EdTech website, Z-kai, was endorsed by the Japanese Education Ministry for all elementary, middle, and high school students to learn core subjects during Covid-19 school closures.[73] Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers:

71 Gunes Acar et al., "The Web Never Forgets: Persistent Tracking Mechanisms In the Wild," In Proceedings of CCS 2014, November 2014, https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html (accessed July 7, 2021). See also: Julia Angwin, "Meet the Online Tracking Device That is Virtually Impossible to Block," *ProPublica*, July 21, 2014, https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block (accessed July 7, 2021); Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 7, 2021).

72 Canadian Broadcasting Corporation (CBC), "2020-2021 Annual Report," https://cbc.radio-canada.ca/en/impact-and-accountability/finances/annual-reports/ar-2020-2021/highlights/financial-highlights (accessed January 13, 2021).

73 Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, "Learning Support Content For Elementary School Mathematics (as of February 8, 3rd Year of Reiwa)" ("小学校算数における学習支援コンテンツ（令和3年2月8日時点）"), https://web.archive.org/web/20210420015931/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00042.html (accessed July 10, 2021); Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, "Learning Support Content For Junior High School Language (as of February 8, 3rd Year of Reiwa)" ("中学校国語における学習支援コンテンツ（令和3年2月8日時点）"), https://web.archive.org/web/20210420000505/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00055.html (accessed July 10, 2021); Government of Japan, Ministry of Education, Culture, Sports, Science and Technology, "Learning Support Content For High School (as of February 8, 3rd Year of Reiwa)" ("高等学校における学習支援コンテンツ（令和3年2月8日時点）"), https://web.archive.org/web/20210710231357/https://www.mext.go.jp/a_menu/ikusei/gakusyushien/mext_00461.html (accessed July 10, 2021).



Human Rights Watch observed Z-kai fingerprinting children in Japan by secretly drawing this image on their web browsers. © 2022 Hye Jung Han/Human Rights Watch

Two such canvas fingerprinting scripts were built and loaded on the Z-kai site by spider.af, a Japanese company that specializes in ensuring that advertisers' intended audiences see their ads.[74]

Z-kai and spider.af did not respond to our request for comment.

It is not possible to determine the intent behind the use of canvas fingerprinting and how it is used by the product it is embedded in. However, none of these eight websites disclosed their use of canvas fingerprinting to their users. In doing so, these companies effectively kept their users in the dark that they were being invisibly identified and followed around the internet by tracking technology that is difficult to avoid or protect against.

This technique is neither proportionate nor necessary for these websites to function or deliver educational content to children. Its use on children in an educational setting infringes upon children's right to privacy.

Tracking Where Children Are

> Just thinking about my whole age group, the amount of data they share is not even funny. Our everyday lives, our locations. So, their whole lives must be in danger if their data is getting sold off. It's really scary.
>
> —Priyanka S., 16, Uttar Pradesh, India[75]

To know where a child is, and when, is to possess information so sensitive that some governments provide special protections against its misuse and the risks of "abduction, physical and mental abuse, sexual abuse and trafficking."[76]

74 Spider.af, "Spider.af," https://web.archive.org/web/20210708001253/https://spideraf.com/intl/en (accessed July 10, 2021).

75 Human Rights Watch interview with Priyanka S., Uttar Pradesh, India, August 2, 2021.

76 See, for example, UK Information Commissioner's Office, "Age Appropriate Design: A Code of Practice for Online Services; 10. Geolocation," September 2, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/ (accessed July 9, 2021);Government of the Republic of Korea, "Location Information Act" ("위치정보의 보호 및 이용 등에 관한 법률"), Act No. 14224, May 30, 2017, https://law.go.kr/LSW/lsInfoP.do?lsiSeq=183644&lsId=009882&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20170530&vSct=&ancYnChk=undefined#0000, art. 26; in 2013, the US Federal Trade Commission revised the country's Children's Online Privacy Protection Act (COPPA), or child-specific data protection law, in part motivated by concerns over the emerging misuse of children's geolocation data. See: Federal Trade Commission, "Children's Online Privacy Protection Rule; Final Rule," 16 CFR Part 312, vol. 87 no. 12, January 17, 2013, p. 3972, https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf (accessed July 9, 2021).

Information about a child's physical location also reveals powerfully intimate details about their life far beyond their coordinates. Mobile phones have the ability to find and track a child's precise physical location over time, including when and how long they were in any given place. Once collected, these data points can reveal such sensitive information as where a child lives and where they go to school, trips between divorced parents' homes, and visits to a doctor's office specializing in childhood cancer.

Even without names or other obviously identifiable information attached to location data, it is startlingly easy to identify real children and people without their awareness or consent. A *New York Times* investigation determined that just two precise location data points is enough to identify a person; journalists were, for example, able to identify a single child and where they live by tracing their daily route from home to school, as well as a middle-school math teacher by her classroom and her doctor's office.[77]

At a time when many children were remotely learning from home under Covid-19 lockdowns, the surveillance of their physical presence through location data likely revealed addresses and places most significant to them.

Apps: Precise Location Data

Of the 73 apps examined by Human Rights Watch, 22 apps (30 percent) granted themselves the ability to collect precise location data, or GPS coordinates that can identify a child's exact location to within 4.9 meters.[78] These 22 apps also had the ability to collect the time of the device's current location, as well as the last known location of the device—revealing exactly where a child is, where they were before that, and how long they stayed at each place.

Of these, 10 apps appear to have the ability to collect precise location data from an estimated 52.1 million children, as these apps' own materials describe and appear to market them for children's use in education. None of these apps apparently designed for use by children disclose to their students that they collect their precise location data.

Four apps are built and owned by the education ministries of India, Indonesia, Iran, and Turkey, giving these governments the ability to track an estimated 29.5 million children and pinpoint where they are, at any given moment, until the app is closed by the user.

77 Stuart A. Thompson and Charlie Warzel, "One Nation, Tracked: Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (accessed July 8, 2021); Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," New York Times, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (accessed July 8, 2021). See also: Charlie Warzel and Stuart A. Thompson, "Where Even the Children Are Being Tracked," New York Times, December 21, 2019, https://www.nytimes.com/interactive/2019/12/21/opinion/pasadena-smartphone-spying.html (accessed July 8, 2021).

78 US National Coordination Office for Space-Based Positioning, Navigation, and Timing, Global Positioning System (GPS), "GPS Accuracy," https://www.gps.gov/systems/gps/performance/accuracy/ (accessed July 8, 2021).

EdTech Product	Country	Apparently designed for use by children?	Developer	GPS	Timestamp of current location	Last known location	Disclosed in privacy policy?	Estimated Users[79]
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Private	Yes	Yes	Yes	Yes	100,000,000
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Private	Yes	Yes	Yes	No	500,000,000
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Private	Yes	Yes	Yes	No	1,000,000
Minecraft: Education Edition	Australia: Victoria	Yes	Private	Yes	Yes	Yes	No	500,000
Threema Work	Germany: Baden-Württemberg, Germany: Bavaria	No	Private	Yes	Yes	Yes	Yes	500,000
Moodle	Germany: Baden-Württemberg, Romania, Kazakhstan	Yes	Private	Yes	Yes	Yes	No	10,000,000
Padlet	Germany: Bavaria, Romania, Colombia	No	Private	Yes	Yes	Yes	Yes	5,000,000
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Private	Yes	Yes	Yes	Yes	10,000,000,000

79 As verified by Google Play Store user installs globally, as of October 2021.

Diksha	India: National	Yes	Government	Yes	Yes	Yes	No	10,000,000
WhatsApp	India: Uttar Pradesh, Cameroon	No	Private	Yes	Yes	Yes	Yes	5,000,000,000
Rumah Belajar	Indonesia	Yes	Government	Yes	Yes	Yes	No	1,000,000
Ruangguru	Indonesia	Yes	Private	Yes	Yes	Yes	No	10,000,000
Sekolah.mu	Indonesia	Yes	Private	Yes	Yes	Yes	No	1,000,000
Shad	Iran	Yes	Government	Yes	Yes	Yes	No	18,000,000
LINE	Japan, Taiwan	No	Private	Yes	Yes	Yes	Yes	500,000,000
Telegram	Nigeria	No	Private	Yes	Yes	Yes	No	1,000,000,000
Taleemabad	Pakistan	Yes	Private	Yes	Yes	Yes	No	1,000,000
Naver Band	Republic of Korea	No	Private	Yes	Yes	Yes	Yes	50,000,000
KakaoTalk	Republic of Korea	No	Private	Yes	Yes	Yes	Yes	100,000,000
Extramarks	South Africa	Yes	Private	Yes	Yes	Yes	No	100,000
Facebook	Taiwan	No	Private	Yes	Yes	Yes	Yes	5,000,000,000
Özelim Eğitimdeyim	Turkey	Yes	Government	Yes	Yes	Yes	No	500,000

These 22 apps gave 18 third-party companies access to children's precise location data, potentially enabling these companies to analyze, trade, and monetize this information.

Of these 22 apps, 20 apps were also found to have the ability to collect coarse location data, which reveals where children are with an accuracy approximately equivalent to a city block.[80] Such data can also be used to infer intimate details about a child; research scientists have concluded that just four approximate, anonymous location data points is enough to re-identify 95 percent of individuals.[81]

Human Rights Watch did not find evidence that precise location data was used to provide core app functionality or any educational benefit to children.

When reached for comment, Cisco stated that Webex does not collect users' precise location, last known location or coarse location, or their call logs.

80 Google Maps Platform, "Location Data," July 1, 2021, https://web.archive.org/web/20210708220829/https://developers.google.com/maps/documentation/android-sdk/location (accessed July 8, 2021).

81 Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," *Nature Scientific Reports* vol. 3 (2013), accessed June 30, 2021, doi:10.1038/srep01376.

Case Study: Diksha, India

Diksha is an EdTech app owned and operated by India's Education Ministry.[82] First launched in 2017 and later used during the pandemic as the government's primary means of delivering online education to students, Diksha offers lessons, textbooks, homework, and other educational material for grades 1 to 12. Diksha was downloaded by over 10 million students and teachers as of 2020. To drive further adoption, some state education ministries set quotas for government teachers to compel a minimum number of their students to download the app.[83]

Human Rights Watch found that Diksha collects children's precise location data, including the date and time of their current location and their last known location. However, the Indian government does not disclose through Diksha's privacy policy or elsewhere that it collects children's location data. Instead, it misleadingly states that Diksha collects a different piece of information—a user's IP address—only once, "for the limited purpose of determining your approximate location – the State, City and District of origin… and the precise location of any User cannot be determined."[84]

Diksha also granted access to its students' location data to Google, through the two SDKs—Google Firebase Analytics and Google Crashlytics—embedded in the app. Through dynamic analysis, Human Rights Watch observed Diksha collecting and transmitting children's AAID to Google. It appears that Diksha shares children's personal data with Google for advertising purposes.

India's Education Ministry, as well as the state education ministries of Maharashtra and Uttar Pradesh, which had endorsed the use of Diksha, did not respond to requests for comment.

As a result, children and their parents were denied the opportunity to make informed decisions about whether to permit the Indian government to surveil their location and share it with third-party companies.

Wi-Fi SSID

Companies can also track a child's whereabouts by collecting information about the wireless network to which their phone is connected. Because Wi-Fi routers tend to be in fixed locations, collecting the names of wireless networks to which a child has previously connected can reveal places such as their home, school, places of worship, hospitals, addresses of extended family, and other places where a child spends significant time. Such information can then be used to infer more about a child, including their habits and relationships.[85]

To do this, mobile phones collect the Wi-Fi SSID, which yields the name of a Wi-Fi router that the phone is connected to or the name of one nearby. Companies can look up these routers in databases that list where public Wi-Fi locations are located in the world, then map them to precise GPS coordinates.[86]

Human Rights Watch found 18 apps accessing the Wi-Fi SSID. In seven cases, the apps' own materials describe and appear to market them for children's use; two of these are owned and provided by the governments of Iran and Turkey. Seven of these apps do not disclose in their privacy policy that they collect any location data from their users, much less precise location data such as the Wi-Fi SSID.

82 Government of India, Department of School Education & Literacy and Ministry of Human Resource Development, "Remote Learning Initiatives Across India," June 2020, https://www.education.gov.in/sites/upload_files/mhrd/files/India_Report_Digital_Education_0.pdf (accessed May 21, 2021).

83 Ishita Bhatia, "Remote learning: UP sets target, tells each govt teacher to convince 10 students to download Diksha app," The Times of India, November 18, 2020, https://timesofindia.indiatimes.com/city/meerut/remote-learning-up-sets-target-tells-each-govt-teacher-to-convince-10-students-to-download-diksha-app/articleshow/79268507.cms (accessed August 24, 2021).

84 Government of India, Ministry of Education, National Council of Educational Research and Training, "Privacy Policy of Diksha, Version 11," April 28, 2021, https://web.archive.org/web/20210825230434/https://static.diksha.gov.in/privacy-policy/terms-of-use.html (accessed August 25, 2021).

85 See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_0.pdf (accessed April 3, 2021), pp. 11, 18; Jeremy Gillula and Peter Eckersley, "Is Your Android Device Telling the World Where You've Been?" Electronic Frontier Foundation, July 3, 2014, https://www.eff.org/deeplinks/2014/07/your-android-device-telling-world-where-youve-been (accessed July 8, 2021).

86 Wikipedia, "Wi-Fi positioning system," https://en.wikipedia.org/wiki/Wi-Fi_positioning_system (accessed July 8, 2021).

EdTech Product	Country	Apparently designed for use by children?	Developer	Wi-Fi SSID	Disclosed in privacy policy?
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Private	Yes	Yes
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Private	Yes	No
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Private	Yes	Yes
Threema Work	Germany: Baden-Württemberg, Bavaria	No	Private	Yes	Yes
Padlet	Germany: Bavaria, Romania, Colombia	Yes	Private	Yes	Yes
LINE	Japan, Taiwan	No	Private	Yes	Yes
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, , United Kingdom: England	No	Private	Yes	Yes
WhatsApp	India: Uttar Pradesh, Cameroon	No	Private	Yes	Yes
Ruangguru	Indonesia	Yes	Private	Yes	No
Sekolah.mu	Indonesia	Yes	Private	Yes	No
Shad	Iran	Yes	Government	Yes	No
Telegram	Nigeria	No	Private	Yes	No
Taleemabad	Pakistan	Yes	Private	Yes	No
Naver Band	Republic of Korea	No	Private	Yes	Yes
KakaoTalk	Republic of Korea	No	Private	Yes	Yes
Extramarks	South Africa	Yes	Private	Yes	No
Facebook	Taiwan	No	Private	Yes	Yes
Özelim Eğitimdeyim	Turkey	Yes	Government	Yes	Yes

Websites: Coarse Location Data

Every device connected to the internet has an Internet Protocol (IP) address to send and receive data, much like a physical address is needed to send and receive physical mail.[87] Every app or website transmits its users' IP address in the standard course of communicating with an internet server. However, IP addresses can also be used to infer a user's location with coarse granularity, or to identify the country, city, and postal code of the person's location.

While it is not possible to determine from a technical assessment whether a company is using an IP address to determine a user's approximate location, most AdTech companies that Human Rights Watch observed receiving children's IP addresses from government-endorsed EdTech products offer geolocation targeting services based on IP addresses.

Criteo, for example, is an AdTech company that specializes in retargeting ads across the internet at people who have previously visited a given website. Decisions on who to target are made using what the company's CEO called its "powerful flashlight" to identify people online, which is powered by the data it holds on "2.5 billion unique users globally, of which 98 percent have persistent identifiers beyond cookies."[88] The company claims that it has "advanced AI algorithms" which "use [...] over 120 shopping signals to create a unique ad for every user designed to get the highest engagement."[89]

Criteo notes that "Our partners provide us with information about your geographical location derived from your truncated IP address, points of interest that are near you (e.g. stores that are geographically close to you) ... This allows us to improve the relevance of our services by displaying advertisements for products available in your geographical area."[90]

Human Rights Watch observed Criteo receiving children's data and their IP addresses from the EdTech websites Descomplica (Brazil: São Paulo), Escola Mais (Brazil: São Paulo), Study Sapuri (Japan), Z-kai (Japan), 100Ballov (Kazakhstan), Campus.pk (Pakistan), and EBS (Republic of Korea). All of these websites are designed and intended for children's use in education.

In its response, Criteo confirmed that it specializes in behavioral advertising, and that it collects truncated IP addresses to determine a person's location to within one km. While the company stated that it does not intentionally or knowingly collect personal information from children, it confirmed that three of these websites—Descomplica, Study Sapuri, and Z-kai—were current clients and said that it was not currently working with the other four websites. Criteo did not address whether it had received children's data from the EdTech websites listed above.[91]

87 Electronic Frontier Foundation, Surveillance Self-Defense, "IP Address," https://ssd.eff.org/en/glossary/ip-address (accessed July 8, 2021).

88 Megan Clarken, "Edited Transcript: CRTO.OQ – Q2 2020 Criteo SA Earnings Call, July 28, 2020 / 12:00 pm GMT", Criteo, July 28, 2020, https://web.archive.org/web/20210801054221/https://filecache.investorroom.com/mr5ir_criteo/1009/download/CRTO-USQ_Transcript_2020-07-29.pdf (accessed July 31, 2021), p. 5.

89 Criteo, "Criteo AI Engine," https://web.archive.org/web/20210801054934/https://www.criteo.com/technology/ai-engine/ (accessed July 31, 2021).

90 Criteo, "Privacy Policy," November 26, 2020, https://web.archive.org/web/20210825155825/https://www.criteo.com/privacy/ (accessed August 25, 2021); Criteo, "Anatomy of an Ad Set," https://web.archive.org/web/20210826061931/https://developers.criteo.com/marketing-solutions/docs/anatomy-of-an-ad-set (accessed August 25, 2021).

91 Human Rights Watch email correspondence with Maribel Henriquez, Senior Communications Manager, Criteo, April 7, 2022.

Tracking Who Children Know

Finding out who you know has long been considered valuable by advertisers, who recognize that one of the most effective methods of attracting new customers is through referrals made by family, friends, and contacts.[92] The Nielsen Company, a data broker and AdTech company that Human Rights Watch detected receiving children's data from three EdTech websites—Stoodi (Brazil: São Paulo), CBC Kids (Canada), and WeSchool (Italy)—notes that "the most credible form of advertising comes straight from the people we know and trust."[93]

Contact information can also be used for shadow profiling, in which companies siphon data from their users' contacts lists in order to develop profiles on people who have never used their services. Facebook, for example, came under intense scrutiny in a series of high-profile cases for sharing the personal information of its users' friends, without their consent or awareness, between 2010 and 2018.[94] Among others, this enabled Cambridge Analytica, a political firm that claimed to influence people by creating uniquely detailed personality profiles and then tailoring political messaging to them, to collect information not only from the 270,000 users who consented to share their data through Cambridge Analytica's Facebook-linked app, but also from up to 87 million unwitting people listed as their friends on Facebook.[95]

When details about the personal relationships of a child are collected without consent or awareness by the child or by the family member or friend in question, it is an arbitrary intrusion on privacy for both. For the contact, their right to privacy is affected by the "mere collection of personal data" in which they lose control over information, in addition to the risk of experiencing potential misuse of their personal data.[96]

Human Rights Watch identified 18 EdTech apps (25 percent) with the ability to collect information about their users' friends, family, and other acquaintances by accessing the contacts list saved on users' phones. This may have allowed these apps to learn personal details about these contacts, including any saved names, phone numbers, emails, addresses, and relationships ("Grandma," "Dad"). In addition, all of these apps, with the exception of Telegram, had the ability to collect profile photos of the contact, if one had been saved.

Three apps developed specifically for children—Kelas Pintar (Indonesia), Shad (Iran), and Extramarks (South Africa)—do not disclose this practice in their privacy policies. Human Rights Watch found that this data was neither necessary for these apps to function, nor provided educational benefit to children.

92 Google Firebase, "Reward Referrals," July 8, 2021, https://web.archive.org/web/20210709224909/https://firebase.google.com/docs/dynamic-links/use-cases/rewarded-referral (accessed July 9, 2021).

93 "Recommendations From Friends Remain Most Credible Form of Advertising Among Consumers; Branded Websites Are The Second-Highest-Rated Form," Nielsen press release, September 28, 2015, https://web.archive.org/web/20210709224818/https://www.nielsen.com/us/en/press-releases/2015/recommendations-from-friends-remain-most-credible-form-of-advertising/ (accessed July 9, 2021).

94 After declaring that it would no longer share such information with others in 2014, Facebook continued to give third parties access to personal data about its users and their friends. In 2014 and 2015, Facebook struck deals with companies including Netflix, Lyft, and the Royal Bank of Canada, giving them full access to its users' friends' data. In 2018, Facebook was discovered to have given advertisers and device makers access to detailed data on its users' friends—including their relationship status, religious and political leanings, and events they planned to attend—even if their users had denied Facebook permission to do so. See: Government of the United Kingdom, House of Commons, Digital, Culture, Media and Sport Committee, "Disinformation and 'fake news': Interim Report," HC 363, July 29, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf (accessed July 9, 2021), pp. 27-30; Josh Constine, "Facebook is Shutting Down Its API For Giving Your Friends' Data To Apps," *TechCrunch*, April 28, 2015, https://techcrunch.com/2015/04/28/facebook-api-shut-down/ (accessed July 9, 2021); Giridhari Venkatadri et al., "Investigating Sources of PII Used in Facebook's Targeted Advertising," *Proceedings On Privacy Enhancing Technologies*, vol. 2019, no. 1 (2018), accessed July 9, 2021, doi: 10.2478/popets-2019-0013, pp. 227-244; Kashmir Hill, "Facebook Is Giving Advertisers Access To Your Shadow Contact Information," *Gizmodo*, September 26, 2018, https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051 (accessed July 9, 2021); Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York Times*, June 3, 2018, https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html (accessed July 10, 2021).

95 Facebook, "An Update On Our Plans To Restrict Data Access On Facebook," April 4, 2018, https://about.fb.com/news/2018/04/restricting-data-access/ (accessed July 9, 2021).

96 UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, para. 7.

These 18 apps may have granted access to their users' contact data to 16 third-party companies.

EdTech app	Country	Apparently designed for use by children?	Contacts' details	Contacts' photos	Ed Tech app may give access to:
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	No	Yes	Yes	Google Firebase Analytics, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes
Cisco Webex	Australia: Victoria, Japan, Poland, Spain, Republic of Korea, Taiwan, US: California	No	Yes	Yes	Google Firebase Analytics, Google Crashlytics, Amplitude
Zoom	Australia: New South Wales, Cameroon, Kazakhstan, Republic of Korea, Romania, US: California, Texas, United Kingdom: England	No	Yes	Yes	Google Firebase Analytics
Remind	Colombia	Yes	Yes	Yes	Google Firebase Analytics, Google Crashlytics, Braze, Pusher
Dropbox	Colombia	No	Yes	Yes	Google Firebase Analytics, Adjust, Bugsnag
Padlet	Germany: Bavaria, Romania, Colombia	No	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Branch, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	No	Yes	Yes	Google Firebase Analytics, Google AdMob
WhatsApp	India: Uttar Pradesh, Cameroon	No	Yes	Yes	Google Analytics

Kelas Pintar	Indonesia	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager, Facebook Analytics, Facebook Login, Facebook Share, Adjust
Shad	Iran	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics
LINE	Japan, Taiwan	No	Yes	Yes	Google Analytics, Google AdMob, Facebook Login, Facebook Share
Telegram	Nigeria	No	Yes	No	Google Firebase Analytics
Edmodo	Nigeria, Egypt, Colombia, Ghana, Romania, Thailand	Yes	Yes	Yes	Google Crashlytics, Google Firebase Analytics, Google AdMob, JW Player, Matomo
Naver Band	Republic of Korea	No	Yes	Yes	Google Firebase Analytics, Google AdMob, AppsFlyer, Facebook Analytics, Facebook Login, Facebook Share, InMobi, Moat
KakaoTalk	Republic of Korea	No	Yes	Yes	Google Firebase Analytics, Google Crashlytics, AdFit
Extramarks	South Africa	Yes	Yes	Yes	Google Analytics, Google Firebase Analytics, Google AdMob, Google Tag Manager, Adjust, Facebook Login, Facebook Places, Facebook Share
Google Meet	Spain, Poland, Taiwan, US: California, Texas	No	Yes	Yes	Google Firebase Analytics
Facebook	Taiwan	No	Yes	Yes	N/A

Tracking What Children Do in the Classroom

Human Rights Watch found that many governments enabled third-party companies to infringe on children's privacy by allowing them to conduct unnecessary, disproportionate surveillance on what children do in their virtual classrooms. Using tracking technologies invisible to their users, many EdTech companies examined in this report collected and sent this data to AdTech and related companies, who in turn enabled a sprawling network of advertisers and other companies to use children's data for commercial purposes, and exposed children to further risk of misuse and exploitation of their data.

Children and parents were denied the knowledge or opportunity to challenge these practices. Most EdTech companies did not disclose their surveillance of children and their data; similarly, most governments did not provide notice of these practices and their risks to students or teachers when announcing their endorsements of EdTech platforms.

But even if children were aware of being surveilled in their virtual classrooms, they could not meaningfully opt out or refuse to provide their personal data to EdTech companies. The Council of Europe noted, "[A]s the education is compulsory and refusal or withdrawal of consent could be detrimental to the development of the child, children would not be in a position to consent freely, irrespective of the assistance by parents or legal representatives."[97] This was particularly true in countries that provided most children's education solely through officially-endorsed EdTech platforms, as further discussed in Chapter 4.

Websites: Ad Trackers

Ad trackers identify and collect information about a person visiting a website. By scrutinizing a person's every action and behavior, ad trackers use their presumed preferences to target them with specific ads, then measure how successful the ad has been at capturing the person's attention or enticing them to click on it.[98]

Ad trackers usually take the form of JavaScript scripts or web beacons, which are near-invisible, 1x1 pixel images that are hidden on a website to silently record what users do, including when they visited the site and where they were physically located.[99]

97 "Contribution prepared by the Secretariat of the Council of Europe on the subject of the right to privacy of children, in response to the consultation carried out by the UN Special Rapporteur on the right to privacy (UNSRP)," October 5, 2020, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/privacy-child/Regional-Org-and-UN/1-CoE.docx (accessed August 3, 2021), pp. 3, 4.

98 Surya Mattu and Aaron Sankin, "How We Built a Real-Time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 10, 2021).

99 Ibid

A 1x1 pixel image placed in the center of this page.

Human Rights Watch found that children's educational websites installed as many third-party trackers on personal devices as do the world's most popular websites aimed at adults. Out of a total 125 EdTech websites, 113 websites (90 percent) placed third-party trackers on devices and browsers used by children. In comparison, an investigation conducted by The Markup in September 2020 found that of the world's over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, 84.9 percent loaded third-party trackers on their website.[100]

Put another way, children are just as likely to be surveilled in their virtual classrooms as adults shopping in the world's largest virtual malls, if not more so.

Children are also being tracked at dizzying scale. Human Rights Watch found 724 third-party trackers embedded in these EdTech websites; a child logging into a single one of these 113 platforms at the start of the school day could expect to be tracked by an average of 7 third-party trackers. One EdTech site, Z-kai, endorsed by the Japanese Education Ministry for all elementary, middle, and high school students in Japan to learn core subjects during Covid-19 school closures, embedded 54 ad trackers that were detected transmitting students' data to 37 companies, predominantly in AdTech.

The number of advertising or other third-party companies receiving children's data was discovered to be even greater than the number of EdTech companies sending this data to them. Human Rights Watch detected these 113 websites transmitting children's data to 161 companies.

Out of the 125 websites analyzed by Human Rights Watch, just 13 websites (10 percent) did not collect and transmit data about children through third-party trackers. These were: Juana Manso (Argentina), Stile Education (Australia: Victoria), Zoom (Australia: New South Wales; Cameroon; Kazakhstan; Republic of Korea; Romania; United States: California, Texas; United Kingdom: England), Faso e-Educ@tion (Burkina Faso), Learn (Canada: Quebec), Biblioteca Digital Escolar (Chile), Jules (France), Ma classe à la maison (France), MaSpéMaths (France), Mebis (Germany: Bavaria), Visavid (Germany: Bavaria), NHK for School (Japan), and iEN (Saudi Arabia).[101] These sites point to an alternate vision of online education for children, one that preserves their privacy and does not surveil their students for profit.

100 Surya Mattu and Aaron Sankin, "The High Privacy Cost of a 'Free' Website," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites (accessed July 12, 2021); Victor Le Pochat et al., "Tranco," generated on July 13, 2021, https://tranco-list.eu/list/KLPW/1000000 (accessed July 13, 2021); see also, Victor Le Pochat et al., "TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

101 Human Rights Watch did not include Facebook in this list; while the website version of the product was not found with third-party ad trackers, the company relies on its own first-party tracking tools to collect and send its users' data back to itself. See: Aaron Sankin and Surya Mattu, "I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What's Going On?" *The Markup*, October 1, 2020, https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on (accessed July 13, 2021).

Case Study: EBS, Republic of Korea

At the beginning of the pandemic, the Republic of Korea (South Korea)'s Education Ministry suspended all in-person learning and committed to providing online classes for all primary and secondary school students in the country. Jae-kuk H., a 14-year-old boy in Seoul, told Human Rights Watch at the time: "I feel like the earth has just stopped."[102] By April 20, 2020, the website of the national educational public broadcaster, Korea Educational Broadcasting System (EBS), received on average over 2.1 million users every day.[103]

Human Rights Watch notes that during Covid-19 school closures, the Korean education ministry recommended watching TV broadcast lessons on EBS, and to re-watch recordings of those lessons on the EBS sites. EBS' home page is the primary gateway to access EBS' educational offerings, much of which are directed towards children.[104] Human Rights Watch also notes that it analyzed, among others, specific webpages that the Korean education ministry recommended for primary school students' use.[105]

When a child opens up EBS' home page, or its main page for primary school students, to log into school for the day, a swarm of trackers get to work. Within milliseconds, 24 ad trackers begin to suck up a child's every movement and interaction within the virtual classroom and transmit this information to 15 advertising companies. A few of these recipients are large data brokers, companies that compile digital dossiers about people from information obtained from public, private, online, and offline sources.

EBS Sent Children's Data to 15 AdTech Companies

AdTech Company	AdTech Domain Receiving Children's Data	How the AdTech company uses the data it receives, based on its marketing materials
ADPIE	adpies.com	"Generate amazing ad revenue like never before."[106]
Appier	appier.net	"Achieve hyper-personalization and deliver 1:1 recommendations … Engage your customers with real-time notifications triggered by their behavior."[107] "[U]nifies and enriches existing customer data to help you better understand your audience and run AI models to easily predict their future actions."[108]

102 Human Rights Watch interview with Jae-kuk H., 14, Seoul, South Korea, June 6, 2020.

103 South Korea's education ministry invested in rapidly expanding learning content on EBS as part of the country's online learning response to Covid-19. See, for example: Korea Education and Research Information Service, "Responding to COVID-19: Online Classes in Korea," June 8, 2020, https://www.keris.or.kr/eng/na/ntt/selectNttInfo.do?mi=1521&nttSn=36647 (accessed August 30, 2021), pp. 5, 9. See also: Republic of Korea Ministry of Education, "Elementary summer vacation, rewarding and together with educational broadcast EBS!" ("초등 여름 방학, 보람 있게 교육 방송 EBS와 함께!") Republic of Korea Ministry of Education Official Blog, July 29, 2020, https://if-blog.tistory.com/10833 (accessed August 30, 2021); Republic of Korea Ministry of Education, "School postponed due to COVID-19, study at home like this," ("코로나19로 인한 개학연기, 가정에서 이렇게 공부하세요~,") Happy Education (blog), https://happyedu.moe.go.kr/happy/bbs/selectBoardArticleInfo.do?bbsId=BBSMSTR_000000000231&nttId=10765 (accessed August 30, 2021); Danyang Primary School, "Online Learning Guide," ("온라인 학습 안내,") Danyang Primary School website, https://school.cbe.go.kr/_class/board/view/danyang-e/2020/G02020402/383390/9548791?&mode=ma (accessed August 30, 2021)

104 EBS, "EBS," https://www.ebs.co.kr/ (accessed May 22, 2022)

105 Republic of Korea Ministry of Education, "Elementary summer vacation, rewarding and together with educational broadcast EBS!" ("초등 여름 방학, 보람 있게 교육 방송 EBS와 함께!") Republic of Korea Ministry of Education Official Blog, July 29, 2020, https://if-blog.tistory.com/10833 (accessed August 30, 2021); Republic of Korea Ministry of Education, "School postponed due to COVID-19, study at home like this," ("코로나19로 인한 개학연기, 가정에서 이렇게 공부하세요~,") Happy Education (blog), https://happyedu.moe.go.kr/happy/bbs/selectBoardArticleInfo.do?bbsId=BBSMSTR_000000000-231&nttId=10765 (accessed August 30, 2021). For an example of a school which adopted the education ministry's recommendations, see: Danyang Primary School, "Online Learning Guide," ("온라인 학습 안내,") Danyang Primary School website, https://school.cbe.go.kr/_class/board/view/danyang-e/2020/G02020402/383390/9548791?&mode=ma (accessed August 30, 2021)

106 AdPie, "AdPie," https://web.archive.org/web/20210804044228/https://www.adpies.com/en/ (accessed August 3, 2021).

107 Appier, "Aiqua Customer Engagement Platform," https://web.archive.org/web/20210807012038/https://www.appier.com/aiqua-customer-engagement-platform/ (accessed August 3, 2021).

108 Appier, "Aixon, Your Data Science Platform," https://web.archive.org/web/20210807012147/https://www.appier.com/aixon-your-data-science-platform/ (accessed August 3, 2021).

BizSpring	bizspring.net	"BizSpring provides a variety of data solutions for MarTech/AdTech," "'Integrate' and 'connect' all behavioral data centered on 'people.' Predict user intentions with big data in which each individual's behavioral patterns are alive and deliver a message that can directly increase conversion performance."[109] "We build a single customer profile by integrating all data about the customer, including the movements and paths they take in an app or website … and even behavioral data from 3rd parties. Customers with specific behavioral tendencies can be easily identified at the level of each 'person,' and target segments can be extracted in the form of a list according to the purpose and utilized in various marketing activities."[110]
	logger.co.kr	"Logger™ provides data that can maximize marketing performance by tracking … every action that occurs on your website," "Track your visitor's clickstream to understand performance: … tracks all of the activities of visitors online and provides analysis data that can determine ROI."[111]
Criteo	criteo.com, criteo.net	"2.5 billion users … active in 100+ countries: a global perspective of consumers and commerce."[112] "Pooled identity data within Criteo Shopper Graph ensures accurate cross-device identification from the billions of active online shoppers who use multiple devices to shop, and the tens of thousands of websites worldwide that continuously share their data with us. Stitch together device identifiers across billions of user timelines. Find patterns of behavior and listen to signals of intent."[113]
Dable	dable.io	"Improve traffic and advertising earnings with the best personalization platform in Asia," "consider personalization technology and native ads as effective profit models in increasing preference and user attention. Detailed targeting by interest, region, medium, time of day, etc."[114]
Enliple	mediacategory.com	"Enliple's advertising solution differentiator is to analyze customer behavior data through Big Data-based customer insight and to deliver more personalized predictive analytics and maximize user's ROI by automatically learning real-time customer behavior."[115]

109 MarTech is an advertising industry term for marketing technology. See: BizSpring, "Solution," https://web.archive.org/web/20210410200024/http://bizspring.co.kr/company/solution.php (accessed August 3, 2021).

110 BizSpring, "PeopleDB: Connecting 'People' and 'Data'," https://web.archive.org/web/20210831005229/https://drive.google.com/file/d/1Dcg4nC26lHfIrtCoP7lVgumwe1EUSCSH/view (accessed August 3, 2021), p. 4.

111 Logger, "Marketing," https://web.archive.org/web/20210804050116/https://logger.co.kr/product/marketing/ (accessed August 3, 2021).

112 Criteo, "Criteo," https://web.archive.org/web/20210803001340/https://www.criteo.com/ (accessed August 3, 2021).

113 Criteo, "Shopper Graph," https://web.archive.org/web/20210826020928/https://www.criteo.com/technology/shopper-graph/ (accessed August 3, 2021).

114 Dable, "Dable," https://web.archive.org/web/20210813180914/https://dable.io/en/ (accessed August 3, 2021).

115 Enliple, "Company Overview," https://web.archive.org/web/20200628172500/http://enliple.com/eng/doc/corp (accessed August 30, 2021).

Facebook	facebook.com, facebook.net	"We will use Business Tool Data … to match the Contact Information against user IDs," "to prepare reports on your behalf on the impact of your advertising campaigns and other online content ("Campaign Reports") and (b) to generate analytics and insights about people and their use of your apps, websites, products and services," "to target your ad campaigns to people who interact with your business," "use the Matched User IDs and associated Event Data to help you reach people with transactional and other commercial messages on Messenger and other Facebook Company Products," and "to improve ad delivery, personalize features and content and to improve and secure the Facebook products."[116]
Google	google-analytics.com, doubleclick.net, googleadservices.com, goooglet agmanager.com, google.com	"Easily integrate and access your data to gain a deeper understanding of your customers and identify your most valuable audiences."[117] "Drive engagement with richer, more relevant ads. Thanks to Google's unique understanding of customer intent, you'll be able to show more relevant, meaningful ads to people when they're most interested to learn more about your products and services."[118]
IPONWEB GmbH	bidswitch.net	"BidSwitch creates value for the Ad Tech ecosystem … provides the underlying infrastructure that normalizes the connections between different programmatic technology platforms…. BidSwitch is continuously processing, filtering for fraud & classifying inventory opportunities, layering on data and other services, then intelligently distributing it to relevant buyers across more than 130 Demand Side Technology platforms – all in real-time."[119] "Features: User & ID syncing, Centralized cookie syncing and ID tables."[120]
Kakao	daum.net	"With Kakao's technology, it finds suitable users and displays advertisements by capturing the moments when advertisements are needed. Experience a variety of sophisticated targeting, such as demographics, audience behavior, interests, Kakao services, and current location."[121]

116 Facebook, "Facebook Business Tools Terms," August 31, 2020, https://web.archive.org/web/20210728002513/https://www.facebook.com/legal/terms/businesstools (accessed July 28, 2021).

117 Google, "Google Marketing Platform," https://marketingplatform.google.com/about/enterprise/ (accessed July 28, 2021).

118 Google, "About Discovery Campaigns," Google Ads Help, https://web.archive.org/web/20210921003622/https://support.google.com/google-ads/answer/9176876?hl=en&ref_topic=10307857 (accessed September 20, 2021).

119 Bidswitch, "Smart Infrastructure for Programmatic Platforms," https://web.archive.org/web/20210815033808/https://www.bidswitch.com/technology/ (accessed August 15, 2021).

120 Bidswitch, "Efficient Solutions for Managing Programmatic Supply," https://web.archive.org/web/20210810024525/https://www.bidswitch.com/solutions/dsps/ (accessed August 15, 2021).

121 Kakao, "Display Ads for Business," https://web.archive.org/web/20200809234639/https://business.kakao.com/info/displayad/ (accessed August 15, 2021).

MediaMath	mathtag.com	"MediaMath is the demand-side platform that offers the most powerful off-the-shelf and custom capabilities for brands to reach and influence customers and prospects on any screen. [T]he digital advertising platform offers … different targeting to drive a variety of goals/KPIs: audience, contextual, … location." "Identity Management: Use our flexible identity core to transact directly on a variety of common ID systems. Consumer Segmentation: Build larger and better performing audiences with our deep segmentation tool that marries data from brands/partners with MediaMath data and third-party data." "Easily activate native advertising [which] … matches the form and function of the location in which it appears, providing a more seamless, higher-quality experience on the open Web for consumers." [122]
Naver	naver.com, naver.net	"Naver's performance-based display advertising converts digital consumers into customers: Quickly find potential customers who can better respond to your brand message through a variety of targeting combinations, including gender, age, region, interests, and device OS."[123]
Oracle	bkrtx.com, bluekai.com	See below.
SK Communications Co. Ltd	nate.com	"Based on users' data, intensively focus on your key targets by: gender, age, location, and time." "Collect data that can identify people's tendencies, such as their internet searches, news/posts browsed, shopping, videos viewed, memberships, etc., to find your targets for selective exposure."[124]
WiderPlanet	widerplanet.com	See below.

Among these, Human Rights Watch detected EBS transmitting children's data to Oracle's BlueKai Data Management Platform, a data broker that has amassed one of the world's largest troves of data on people online.[125] The company helps advertisers build even more extensive profiles on their users with the "actionable audience data" it has on billions of people, including billions of daily location signals acquired from other data brokers.[126]

In June 2020, TechCrunch reported that BlueKai had left one of its servers unprotected, spilling data on billions of records on people—names, home addresses, other personally identifiable data—out onto the open web for anyone to find.[127] It was considered one of the most significant data security incidents of 2020, due to the immense size of the exposed database.[128] Human Rights Watch detected EBS sending children's data to Oracle's BlueKai through its ad trackers **bluekai.com** and **bkrtx.com**, both before and after the reported data breach.

122 MediaMath, "Future-Proofed Digital Advertising Platform," https://web.archive.org/web/20210807015327/https://www.mediamath.com/platform/ (accessed August 15, 2021).

123 Naver, "Naver Performance Display Advertising" ("네이버 성과형 디스플레이 광고"), https://web.archive.org/web/20210920231627/https://displayad.naver.com/adplatform (accessed September 20, 2021).

124 SK Communications, "Nate Ads Product Introduction" ("nate 광고 상품소개서"), July 2020, https://adguide.nate.com/html/download.php?filename=SK커뮤니케이션즈_매체소개서_20.07.pdf, pp. 37, 39.

125 By one estimate, BlueKai tracks over one percent of all web traffic in the world. See: Cliqz, Who Tracks Me, "BlueKai," https://whotracks.me/trackers/bluekai.html (accessed July 12, 2021); Bennett Cyphers and Gennie Gebhart, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance," Electronic Frontier Foundation, December 2, 2019, https://www.eff.org/wp/behind-the-one-way-mirror (accessed July 12, 2021).

126 Oracle, "Oracle Data Marketplace," https://web.archive.org/web/20210804031326/https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html (accessed August 3, 2021); Oracle, "2019 Data Directory," https://web.archive.org/web/20210403010855/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf (accessed August 3, 2021). Prominent location data brokers, including PlaceIQ (p. 118), Factual (p. 59), Cuebiq (p. 43), Gravy Analytics (p. 65) make their precise geolocation data available for sale through Oracle Data Cloud's BlueKai marketplace. See also: Privacy International, "Oracle's PlaceIQ acquisition connects physical and digital tracking," July 13, 2016, https://privacyinternational.org/examples/2385/oracles-placeiq-acquisition-connects-physical-and-digital-tracking (accessed August 3, 2021). In 2016 and 2017, Oracle claimed through its marketing materials that its data marketplace contained 5 billion global consumer profiles. See: Oracle, "Get to the Heart of the Matter, the Heart of Your Consumer," 2016, https://web.archive.org/web/20210804032442/https://www.oracle.com/assets/brochure-data-driven-marketing-odc-2894231.pdf (accessed August 3, 2021), p. 10; Nick Whitehead, "Smart Investments in a Data Cloud Strategy," post to "Oracle Analytics" (blog), October 3, 2017, https://web.archive.org/web/20210804032618/https://blogs.oracle.com/analytics/post/smart-investments-in-a-cloud-data-strategy (accessed August 3, 2021).

127 Zack Whittaker, "Oracle's BlueKai Tracks You Across the Web. That Data Spilled Online," *TechCrunch*, June 19, 2020, https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (accessed July 12, 2021).

128 Ibid.

When reached for comment, Oracle confirmed the data leak, and said that an investigation it conducted in 2020 did not uncover evidence that data relating to children were involved. Oracle stated that any receipt of data related to children would be a violation of Oracle's agreements and policy, and did not address whether it had nonetheless received child users' data from six EdTech websites, including EBS. The company did not address whether data received from EBS were exposed as part of the 2020 security breach, and whether it had informed EBS or the other EdTech websites about the security breach.[129]

EBS also sent information about children's behavior in its virtual classrooms to WiderPlanet, a Korean AdTech company. WiderPlanet advertises its "targeted advertising service" powered by the personal data they hold on "99% of Korean internet users" and information on what they do online. The company also claims it can uniquely identify 43 million people, "their interests and demographic types."[130] Given that 96 percent of Korea's population uses the internet, this claim would mean that WiderPlanet holds the personal data of almost the entire country's population.

WiderPlanet did not respond to our request for comment.

EBS' privacy policy notes that it collects and uses its users' personal information for "marketing and advertising," including "demographic analysis, analysis of service visits and usage records, and provision of customized services based on personal information and interests."[131] It does not disclose the use of ad trackers on the site. Nor are the AdTech companies detected by Human Rights Watch to receive children's data disclosed in the list of third parties officially recognized as processors of EBS users' personal data.[132]

In their response to Human Rights Watch, EBS noted that EBS' home page, "while it offers some paid subscription services such as health sciences and cooking classes for adults, mainly functions as a gateway to various Internet education websites of EBS." EBS also stated that, of the user data it sends AdTech companies, it does not send information that would identify children. EBS pointed to a website, EBS Online Class, that it opened with support from the government and provided free education during the Covid-19 pandemic, and stated that this website,which Human Rights Watch did not analyze, as it required a student login, did not share users' data with third-party companies.[133]

Websites: Session Recording, Key Logging

Some EdTech websites are even more intrusive, embedding a tracking technology known as session recording that allows a third party to watch and record all of a user's behavior on a web page.[134] That includes mouse movements, clicks, movements around the page, and anything a user types into the page, even if they don't click submit. The collection of such data minutiae is the digital equivalent of logging video surveillance each time a child scratches their nose or grasps their pencil in class.

Typically, these data would then be scrutinized by the third-party companies that offer session recording services on behalf of the website using their services in order to guess at a child's personality, their preferences, and what they're likely to do next.

129 Human Rights Watch email correspondence with Dorian Daley, Executive Vice President and General Counsel of Oracle, April 15, 2022.

130 WiderPlanet, WiderPlanet," https://web.archive.org/web/20210713204827/https://www.widerplanet.com/?lang=en (accessed July 13, 2021).

121 EBS, "Privacy Policy" ("개인정보처리방침"), February 8, 2021, https://web.archive.org/web/20210804035422/https://sso.ebs.co.kr/policy/privacy?date=20210208&tab=2&ver=%2Fpolicy%2Fprivacy%3Fdate%3D20210208&fsdc= (accessed March 2, 2021), section 1(3), (4).

132 Ibid., sections 4 and 5.

133 Human Rights Watch email correspondence with Suh Dong Won, Policy Planning Center Public Relations Manager of EBS, May 20, 2022.

134 A 2017 study by Princeton researchers found that session recorders were collecting sensitive information such as passwords and credit card numbers. See: Steven Englehardt, Gunes Acar, and Arvind Narayanan, "No boundaries: Exfiltration of personal data by session-reply scripts," post to "Freedom to Tinker" (blog), November 15, 2017, https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/ (accessed July 12, 2021).

Human Rights Watch found 23 EdTech websites, endorsed by eight governments, using session recorders. For all but one, their own materials describe and appear to market them for children's use in education. Most transmitted children's data to the third-party companies Hotjar or Yandex. Hotjar describes itself as a "Product Experience Insights software company". Yandex, a technology company that describes itself as a "technology company that builds intelligent products powered by machine learning," including search and information services, navigation products, and other mobile applications, claims that "clicks, scrolls, keystrokes, and mouse movements are all recorded in a single informative movie... Never miss something interesting with up to 150,000 recordings per day." [135]

When reached for comment, both Hotjar and Yandex answered without responding to our questions. Amazon, who owns cloudfront.net, did not respond to a request for comment.[136]

EdTech Product	Country	Apparently designed for use by children?	Session recorders
Descomplica	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
DragonLearn	Brazil: São Paulo	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Manga High	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
Stoodi	Brazil: São Paulo	Yes	script.hotjar.com, static.hotjar.com
WorkFlowy	Colombia	Yes	script.hotjar.com, static.hotjar.com
iMektep	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Kundelik	Kazakhstan	Yes	mc.yandex.ru/metrika/tag.js, mc.yandex.ru/metrika/watch.js
Daryn Online	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/tag.js
1ooballov	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
iTest	Kazakhstan	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
EdPuzzle	Romania	Yes	script.hotjar.com, static.hotjar.com
ExamenulTau	Romania	Yes	script.hotjar.com, static.hotjar.com
Miro	Romania	No	script.hotjar.com, static.hotjar.com
ȘcoalaIntuitext	Romania	Yes	script.hotjar.com, static.hotjar.com
My School is Online	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js
Digital Lessons	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js

135 Yandex.Metrica, "Behavioral Analytics," https://web.archive.org/web/20210507175616/https://metrica.yandex.com/about/info/behavior (accessed July 12, 2021).136 Human Rights Watch email correspondence with Louanne Grech, Privacy Lead and Data Protection Office, HotJar, March 24, 2022; and with Yandex press office, April 7, 2022.

136 Human Rights Watch email correspondence with Louanne Grech, Privacy Lead and Data Protection Office, HotJar, March 24, 2022; and with Yandex press office, April 7, 2022.

SberClass	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js
Russian Electronic School	Russia	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
My Achievements	Russia	Yes	mc.yandex.ru/webvisor/, mc.yandex.ru/metrika/watch.js
Moscow Electronic School	Russia	Yes	https://mc.yandex.ru/webvisor, mc.yandex.ru/metrika/tag.js, mc.yandex.ru/metrika/watch.js
Sirius	Russia	Yes	mc.yandex.ru/metrika/watch.js
PaGamO	Taiwan	Yes	script.hotjar.com, static.hotjar.com
Kundalik	Uzbekistan	Yes	mc.yandex.ru/metrika/watch.js

A related technique is key logging, a particularly invasive procedure that surreptitiously captures personal information that people enter on forms, like names, phone numbers, and passwords, before they hit submit. This technique has been used for a variety of purposes, including identifying anonymous web users by matching them to postal addresses and real names, before they can consent to anything.[137]

Human Rights Watch detected 16 websites deploying key logging techniques to send children's names, usernames, passwords, and other information to first- and third-party companies. All of these websites, save one, are products whose own materials describe and appear to market them for children's use for education.

EdTech Product	Country	Apparently designed for use by children?	Key loggers
Education Perfect: Science	Australia: Victoria	Yes	hsforms.com
Descomplica	Brazil: São Paulo	Yes	hsforms.com
Manga High	Brazil: São Paulo	Yes	mangahigh.com
Stoodi	Brazil: São Paulo	Yes	veinteractive.com, stoodi.com.br
Aprendo en Línea	Chile	Yes	nullcurriculumnacional.cl
Educar Ecuador	Ecuador	Yes	recursos.educarecuador.gob.ec
Mineduc Digital	Guatemala	Yes	mineduc.gob.gt
Daryn Online	Kazakhstan	Yes	yandex.com
Notesmaster	Malawi	Yes	youtube.com
EBS Online Classes	Republic of Korea	Yes	nullebs.co.kr

137 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," The Markup, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 12, 2021); Surya Mattu and Kashmir Hill, "How a Company You've Never Heard of Sends You Letters About Your Medical Condition," Gizmodo, June 19, 2017, https://gizmodo.com/how-a-company-you-ve-never-heard-of-sends-you-letters-a-1795643539 (accessed July 12, 2021).

Edpuzzle	Romania	Yes	workable.com
Miro	Romania	No	realtimeboard.com
Moscow Electronic School	Russia	Yes	yandex.ru
My School is Online	Russia	No	yandex.ru
Digital Lessons	Russia	Yes	yandex.ru
ST Math	US: Texas	Yes	hsforms.com

For example, Stoodi, an educational website recommended by Brazil's São Paulo Education Ministry, was found using key logging to capture children's names and what they searched for inside of Stoodi. Even if children changed their minds and decided not to submit their personal information, the captured data was still automatically sent to a third-party advertising company, Ve Global.[138] Stoodi did not disclose in its privacy policy that children's data would be captured through key logging, or that it would be sent to a third-party company for commercial use.

Brazil_Stoodi_VPN_inspection.json


```
    ],
    "key_logging": {
      "veinteractive.com": [
        {
          "filter": [
            "IdaaaaTarbell",
            "Tarbell",
            "Idaaaa",
            "IdaaaaTarbell"
          ],
          "match_type": [
            "plaintext"
          ],
          "post_data": "{\"captureUrl\":\"stoodi.com.br/cadastro/\",\"capturedDataContext\":
{\"pageIdentification\":{\"pageType\":0,\"inferred\":{},\"configuredForms\":[1],\"formMappingInfo\":{\"1\":
{\"249605\":{\"type\":44,\"domEventId\":5}}},\"saleFlags\":{\"inferred\":false,\"pixel\":false,
\"identified\":false,\"total\":\"\"}},\"isPageView\":false,\"url\":{\"location\":\"https://www.stoodi.com.br/
cadastro/\",\"referrer\":\"\"},\"jump\":{\"pageJump\":8,\"pageJumpIn\":3}},\"customerId\":1016849,
\"formMappings\":{\"249605\":\"IdaaaaTarbell\"},\"ifsStatus\":{\"audit\":{\"isCookieAvailable\":true,
\"isStorageAvailable\":true,\"message\":\"\"},\"state\":
{\"veCookieId\":\"2f8ae8fe-7eec-4721-b481-464105088454\",\"veCookieStatus\":1}},
\"journeyCode\":\"F59B2BA4-1E96-4CCB-BAA0-F40CFBCB99EF\",\"pageId\":\"1623479368085\",
\"sessionId\":\"28f98471-80b0-45a0-8df1-9aee4d7b44bc\",\"translatorDetected\":false,\"type\":\"pageViewed\",
\"version\":\"v001\"}",
          "post_request_url": "https://dtrcusa.veinteractive.com/FormMappings",
          "post_request_ps": "veinteractive.com"
        },
```


Evidence of Stoodi deploying key logging to send user data to Ve Global, captured in real time. Here, "Idaaaa Tarbell" is the first and last name of a fictional student interested in signing up for Stoodi's services. Once a child types in their name into Stoodi's website, Stoodi immediately captures their name (as seen here under "filter") and sends it to the web address "https://dtrcusa.veinteractive.com/FormMappings." The domain veinteractive.com is owned by the company Ve Global. © 2022 Hye Jung Han/Human Rights Watch

When contacted for comment, Ve Global acknowledged that Stoodi was a former client, and confirmed that Stoodi still had Ve Global's active tracking tags embedded on its website. Ve Global confirmed that it had subsequently disabled the content of the tag.[139] This renders the tracker unusable for Stoodi to continue sending user data to Ve Global.

Stoodi did not respond to our request for comment.

138 Ve Global, formerly known as Ve Interactive, is a "technology company … that provides advertising and marketing solutions" which "helps sell products." See: Ve, "Privacy Policy," https://web.archive.org/web/20210809024159/https://www.ve.com/legal/privacy-policy (accessed August 9, 2021); PitchBook, "Ve Global," https://pitchbook.com/profiles/company/65416-69#overview (accessed August 9, 2021).

139 Human Rights Watch email correspondence with Barbara Lacourt, Director, Global Head of Legal, Ve, March 24, 2022.

Apps: Software Development Kits (SDKs)

For children who attend online classes using their mobile phones, companies are able to track what they do by embedding software development kits (SDKs) in their apps. Much like building blocks in a toy set, SDKs are blocks or libraries of code written by a third-party company that perform defined functions—like a login page, or notification popups—that app developers can conveniently use when building their app without having to create the functionality from scratch. SDKs are the primary means for app developers to enable an app to work with third-party services.

While some SDKs provide core functionality that is needed for an app to work or to improve its technical performance, others are designed solely for advertising—to track users' actions within the app, guess at their preferences, and display the most persuasive ad at the most persuasive time. Still other SDKs provide tracking services that are designed to secretly collect data about the user that can later be compiled and sold. What an SDK does, once implemented in an app, will depend on how it was designed by the third party. SDKs do not fall into neat categories at the time of this writing; for example, an SDK for an analytics company may also facilitate the preparation of user profiles, and an SDK for an advertising company may provide reporting and analytics capabilities.

When a child installs an app for school, the SDKs that the developer embedded in the app also receive the same access as the app to the mobile phone's data and system resources; this facilitates the transmission of the child's personal data directly to the third-party company that owns that SDK.[140]

Human Rights Watch identified 246 SDKs embedded within 66 apps, giving access to a significant array of children's personal data to 36 third-party companies, many of which appear to have primary businesses in advertising and the monetization of users' personal data. It is not possible for Human Rights Watch to reach definitive conclusions as to the companies' motivations in embedding these SDKs, beyond reporting on what it observed in the data and the companies' and governments' own statements.

In the table below, Human Rights Watch lists the third-party SDKs found embedded in each EdTech app, and the "dangerous" permissions and sensitive user data to which they were granted access.[141]

Human Rights Watch notes that it does not conclusively determine how any given SDK is used by a specific app, and that some SDKs may provide multiple capabilities in addition to advertising. Human Rights Watch also notes that the use of "dangerous" permissions to access sensitive data is not inherently unsafe, but poses risks to users' privacy if there are no safeguards that protect against the abuse of such access by the host app or its embedded third-party SDKs.[142]

140 In research commissioned by the Australian Competition and Consumer Commission, security researchers from AppCensus conducted dynamic analysis on 1,000 of the most popular mobile Android apps in Australia, and found that "in many cases, app developers request more permissions than their apps actually need, which puts user data at risk of being accessed by third-party SDKs unnecessarily." See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_0.pdf (accessed April 3, 2021), pp. v, 21.

141 Android labels permissions as "dangerous" when granting that permission to an app can "potentially affect the user's privacy or the device's normal operation," because the app "wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps." See: Android Developers, "Permissions overview," May 7, 2020, https://web.archive.org/web/20200712090715/https://developer.android.com/guide/topics/permissions/overview (accessed April 24, 2022).

142 See, for example, Patrick McGee, "Russian tech giant Yandex's data harvesting raises security concerns," *Financial Times*, March 29, 2022, https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb (accessed April 24, 2022).

EdTech app	Country	SDKs	EdTech app may give a third-party company access to a user's:
Microsoft Teams	Australia: New South Wales, Germany: Bavaria, Republic of Korea, Spain, Taiwan, United Kingdom: England, US: Texas	**Google**: Google Firebase Analytics **Microsoft**: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), call log, camera, microphone
Adobe Connect	Australia: New South Wales	**Google**: Google Analytics	Phone number
Minecraft: Education Edition	Australia: Victoria	**AppLovin**: AppLovin **AppsFlyer**: AppsFlyer **Facebook**: Facebook Ads **Google**: Google AdMob **ironSource**: ironSource **Twitter**: Twitter MoPub **Unity**: Unity3d Ads	Persistent identifiers (Android Advertising ID, Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location
Centro de Mídias da Educação de São Paulo	Brazil: São Paulo	**Google**: Google Crashlytics, Google Firebase Analytics	Camera, microphone
Descomplica	Brazil: São Paulo	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob **Facebook**: Facebook Analytics, Facebook Login, Facebook Places, Facebook Share **MixPanel**: MixPanel	Persistent identifiers (Android Advertising ID), camera
Explicaê	Brazil: São Paulo	**Google**: Google Crashlytics, Google Firebase Analytics Facebook: Facebook Analytics, Facebook Login	Camera
Stoodi	Brazil: São Paulo	**Google**: Google Crashlytics, Google Firebase Analytics, Google Tag Manager, Google Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share **Segment**: Segment	Persistent identifiers (Android Advertising ID, IMEI)
Math Kids	Canada: Quebec	None	N/A

Prof Multi	Canada: Quebec	**Microsoft**: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes	Microphone
Storyline Online	Canada: Quebec	**Google**: Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Biblioteca Digital Escolar	Chile	**Google**: Google Crashlytics, Google Firebase Analytics, Google Analytics	N/A
Dropbox	Colombia	**Google**: Google Firebase Analytics **Adjust**: Adjust **Bugsnag**: Bugsnag	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), camera
Remind	Colombia	**Google**: Google Crashlytics, Google Firebase Analytics **Braze**: Braze **Pusher**: Pusher	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), call log, camera, microphone
WorkFlowy	Colombia	**Google**: Google Firebase Analytics	Camera, microphone
Jules	France	None	N/A
Jitsi	Germany: Baden-Württemberg	**Google**: Google Crashlytics, Google Firebase Analytics	Camera, microphone
Threema Work	Germany: Baden-Württemberg, Germany: Bavaria	**None**	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
Moodle	Germany: Baden-Württemberg, Romania, Kazakhstan	**Google**: Google Firebase Analytics	Precise location (GPS, time of current location, last known location), coarse location, camera, microphone
IServ	Germany: Bavaria	**Google**: Google Firebase Analytics	N/A
itslearning	Germany: Bavaria	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera
SchoolFox	Germany: Bavaria	**Google**: Google Firebase Analytics	Persistent identifiers (Android Advertising ID)

Padlet	Germany: Bavaria, Romania, Colombia	**Google**: Google Crashlytics, Google Firebase Analytics **Microsoft**: Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Crashes **Branch**: Branch	Persistent identifiers (Android Advertising ID, Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), contacts' information (contacts, contacts' photo), phone number, camera, microphone
Ghana Library App	Ghana	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera, microphone
YouTube	India: Uttar Pradesh, Malaysia, Nigeria, United Kingdom: England	**Google**: Google Firebase Analytics, Google AdMob	Persistent identifiers (Wi-Fi MAC), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
e-Balbharti	India: Maharashtra	None	Phone number
Learning Outcomes Smart Q	India: Maharashtra	**Google**: Google Firebase Analytics	None
Diksha	India: National	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), camera, microphone
ePathshala	India: National	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Top Parent	India: Uttar Pradesh	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob **Facebook**: Facebook Login, Facebook Share, Facebook Places **CleverTap**: CleverTap	N/A
WhatsApp	India: Uttar Pradesh, Cameroon	**Google**: Google Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, SMS logs, camera, microphone, fingerprint
Khan Academy	India: Uttar Pradesh, Pakistan, Nigeria, South Africa	**Google**: Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share	N/A

Kelas Pintar	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob, Google Analytics, Google Tag Manager **Facebook**: Facebook Analytics, Facebook Login, Facebook Share **Adjust**: Adjust	Persistent identifiers (Android Advertising ID, IMEI), contacts' information (contacts, contacts' photo), camera
Quipper	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics, Google Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share **Brightcove**: Brightcove **UXCam**: UXCam **Wootric**: Wootric	Persistent identifiers (Android Advertising ID), camera
Ruangguru	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Places, Facebook Share **AppsFlyer**: AppsFlyer **OneSignal**: OneSignal	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, call logs, camera, microphone, flashlight
Rumah Belajar	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location), coarse location, camera
Sekolah.mu	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login **Snowplow**: Snowplow	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, camera, microphone
Zenius	Indonesia	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share **AppsFlyer**: AppsFlyer **CleverTap**: CleverTap	Camera, microphone

Shad	Iran	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
Newton	Iraq	**Google**: Google AdMob **Flurry**: Flurry	Persistent identifiers (Android Advertising ID)
WeSchool	Italy	**Google**: Google Firebase Analytics **Huawei**: Huawei Mobile Services (HMS) Core **OneSignal**: OneSignal	Persistent identifiers (Android Advertising ID), microphone
NHK for School	Japan	None	N/A
schoolTakt	Japan	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
Study Sapuri	Japan	**Google**: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google AdMob **AppsFlyer**: AppsFlyer **Keen**: Keen **Repro**: Repro	Persistent identifiers (Android Advertising ID)
LINE	Japan, Taiwan	**Google**: Google Analytics, Google AdMob **Facebook**: Facebook Login, Facebook Share	Persistent identifiers (aaaaaWi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone, flashlight, fingerprint
Bilimland	Kazakhstan	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID), camera
Daryn Online	Kazakhstan	**Amplitude**: Amplitude	Persistent identifiers (Android Advertising ID), camera, microphone

Kundelik	Kazakhstan	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob **AppMetrica**: AppMetrica **VKontakte**: VKontakte SDK **Yandex**: Yandex Ad	Persistent identifiers (Android Advertising ID), camera
TelmideTICE	Morocco	None	N/A
Telegram	Nigeria	**Google**: Google Firebase Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts), phone number, call logs, camera, microphone
Edmodo	Nigeria, Egypt, Colombia, Ghana, Romania, Thailand	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob **JW Player**: JW Player **Matomo (Piwik)**: Matomo	Persistent identifiers (Android Advertising ID), contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone
Learn Smart Pakistan	Pakistan	**Google**: Google Firebase Analytics	N/A
Muse	Pakistan	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID, Wi-Fi MAC), microphone
Taleemabad	Pakistan	**Google**: Google Crashlytics, Google Firebase Analytics **Facebook**: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location
KakaoTalk	Republic of Korea	**Google**: Google Crashlytics, Google Firebase Analytics **AdFit**: AdFit	Persistent identifiers (Android Advertising ID, Wi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, SMS logs, camera, microphone

Naver Band	Republic of Korea	**Google**: Google Firebase Analytics, Google AdMob	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), camera, microphone
		Facebook: Facebook Analytics, Facebook Login, Facebook Share	
		AppsFlyer: AppsFlyer	
		InMobi: InMobi	
		Moat: Moat	
Edpuzzle	Romania	**Google**: Google Crashlytics, Google Firebase Analytics	Phone number
Kinderpedia	Romania	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), phone number, call logs, camera, microphone
		Huawei: Huawei Mobile Services (HMS) Core	
		OneSignal: OneSignal	
Miro	Romania	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob	Persistent identifiers (Android Advertising ID), camera
		Branch: Branch	
Moscow Electronic School	Russia	**Google**: Google Crashlytics, Google Firebase Analytics	N/A
My Achievements	Russia	**Google**: Google Crashlytics	
		Facebook: Facebook Analytics, Facebook Login, Facebook Share	Persistent identifiers (Android Advertising ID), camera, microphone
		Flurry: Flurry	
		VKontakte: VKontakte SDK	
iEN	Saudi Arabia	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID), camera
African Storybook	South Africa	None	N/A
Extramarks	South Africa	**Google**: Google Crashlytics, Google Firebase Analytics, Google AdMob, Google Tag Manager	Persistent identifiers (Android Advertising ID, Wi-Fi MAC, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), call logs, SMS logs, camera, microphone
		Facebook: Facebook Places, Facebook Login, Facebook Share	
		Adjust: Adjust	

Google Meet	Spain, Poland, Taiwan, US: California, Texas	**Google**: Google Firebase Analytics	Contacts' information (contacts, contacts' photo), camera, microphone
Nenasa	Sri Lanka	**Google**: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager	Persistent identifiers (Android Advertising ID), camera
		Facebook: Facebook Analytics, Facebook Login, Facebook Share, Facebook Places	
		AppsFlyer: AppsFlyer	
Facebook	Taiwan	None	N/A
PaGamO	Taiwan	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID)
		Facebook: Facebook Analytics, Facebook Login, Facebook Share	
		Amplitude: Amplitude	
Eğitim Bilişim Ağı	Turkey	**Google**: Google Firebase Analytics	Persistent identifiers (Android Advertising ID), phone number, call logs, camera, microphone
Özelim Eğitimdeyim	Turkey	**Google**: Google Crashlytics, Google Firebase Analytics, Google Analytics, Google Tag Manager, Google AdMob	Persistent identifiers (Android Advertising ID), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location
		Facebook: Facebook Login	
		Flurry: Flurry	
		StartApp: StartApp	
Zoom	US: California, Cameroon	**Google**: Google Firebase Analytics	Precise location (GPS, time of current location, last known location, Wi-Fi BSSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call log, camera, microphone
Cisco Webex	US: California, Poland	**Google**: Google Crashlytics, Google Firebase Analytics	Persistent identifiers (Android Advertising ID, IMEI), precise location (GPS, time of current location, last known location, Wi-Fi SSID), coarse location, contacts' information (contacts, contacts' photo), phone number, call logs, camera, microphone
		Amplitude: Amplitude	

143 While the Facebook app was also found without third-party SDKs, Meta is an AdTech company that relies on its own first party tracking technologies to collect and send its users' data to itself. See: Aaron Sankin and Surya Mattu, "I Scanned My Favorite Social Media Site on Blacklight and It Came Up Pretty Clean. What's Going On?" *The Markup*, October 1, 2020, https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on (accessed July 13, 2021).

Schoology	US: Texas	**Google**: Google Crashlytics, Google Firebase Analytics **Flurry**: Flurry	Persistent identifiers (Android Advertising ID), camera
Seesaw	US: Texas, Nigeria	**Google**: Google Crashlytics, Google Firebase Analytics	Camera, microphone

Without significant technical expertise, children cannot know whether third-party SDK integrations are present in their EdTech app. But even if they were aware, none of the 66 apps analyzed by Human Rights Watch allowed their users to decline access to their data by a third-party company.

Six apps did not embed any SDKs, demonstrating that it is possible to build an app to provide education for children without sending their personal information to a third-party company. These apps, and the governments that recommended them, are: Math Kids (Canada: Quebec), Jules (France), e-Balbharti (India: Maharashtra), NHK for School (Japan), TelmideTICE (Morocco), and African Storybook (South Africa).[143]

When reached for comment, Zoom informed Human Rights Watch that "Zoom does not currently use Google Analytics for Firebase SDK. Zoom embeds [sic] the Google Firebase SDK in our app only for the limited purposes disclosed on our subprocessors page – i.e. to send push chat, SMS and PBX (phone call) message notifications on Android phones." However, the Google Analytics for Firebase SDK was still embedded in the version of the Zoom app downloaded by Human Rights Watch and used in our technical assessments.

Human Rights Watch further selected eight apps for in-depth technical (dynamic) analysis, which was conducted by the Defensive Lab Agency. Of these, we examine Ruangguru and Muse here to illustrate how apps can allow third-party companies to surveil what students do in the virtual classroom.

Case study: Ruangguru, Indonesia

Ruangguru is an EdTech app recommended by Indonesia's Ministry of Education and Culture.[144] Built by an Indonesian EdTech company of the same name, the company successfully completed a tenth round of funding in April 2021 after the pandemic drove significant growth in user volume and revenue and led to the company's first fiscal year of profitability since its founding in 2014.[145]

The app is widely used by children in Indonesia. Ruangguru reported that it had 22 million users in 2020, and that a free version of its product offered during the pandemic was used by over 10 million students in Indonesia.[146] The company also stated that "we have also been trusted to partner with 32 (out of 34) Provincial Governments and 326 City and District Governments in Indonesia."[147]

Forensic analysis found that Ruangguru collects personal data from its students, including their location, Android Advertising ID, information about the device they use, and in-app navigation, and transmits this to two companies: AppsFlyer and Facebook.

144 Government of Indonesia, Kementerian Pendidikan dan Kebudayaan (Ministry of Education and Culture), "Ministry of Education and Culture Collaborates with the Private Sector to Prepare Online Learning System" ("Kemendikbud Gandeng Swasta Siapkan Sistem Belajar Daring"), March 15, 2020, https://web.archive.org/web/20210804220824/https://www.kemdikbud.go.id/main/blog/2020/03/kemendikbud-gandeng-swasta-siapkan-sistem-belajar-daring (accessed August 4, 2021).

145 Crunchbase, "Ruangguru: Financials," https://www.crunchbase.com/organization/ruangguru/company_financials (accessed August 5, 2021); Ruangguru, "Ruangguru Secures USD 55 Million New Investment Led by Tiger Global Management," post to "Ruangguru" (blog), April 19, 2021, https://web.archive.org/web/20210805155022/https://www.ruangguru.com/blog/ruangguru-secures-usd-55-million-new-investment-led-by-tiger-global-management (accessed August 5, 2021).

146 Ruangguru, "Ruangguru Secures USD 55 Million New Investment Led by Tiger Global Management," post to "Ruangguru" (blog), April 19, 2021, https://web.archive.org/web/20210805155022/https://www.ruangguru.com/blog/ruangguru-secures-usd-55-million-new-investment-led-by-tiger-global-management (accessed August 5, 2021).

147 Ruangguru, "Press Kit," https://web.archive.org/web/20210805155519/https://www.ruangguru.com/press (accessed August 5, 2021). In November 2019, the Indonesian government appointed the CEOs of seven startups, including Ruangguru, to the newly created position of Presidential Special Staff. In April 2020, Ruangguru became the subject of public controversy over a perceived conflict of interest, when Ruangguru won a significant national contract to provide services to a government social benefits program for the unemployed. See: Eisya A. Eloksari, "Conflict of interest? Public questions government's relationship with start-ups," The Jakarta Post, April 16, 2020, https://www.thejakartapost.com/news/2020/04/16/conflict-of-interest-public-questions-governments-relationship-with-start-ups.html (accessed August 5, 2021); Ihsanuddin, "Belva Devara Resigns from Presidential Special Staff" ("Belva Devara Mundur dari Staf Khusus Presiden"), April 21, 2020, https://nasional.kompas.com/read/2020/04/21/18470591/belva-devara-mundur-dari-staf-khusus-presiden (accessed August 5, 2021).

When a child opens up Ruangguru on their phone, the app immediately begins to track what they do in its virtual classrooms, compiling a log of everything the child does and sees in what is known as "in-app navigation." This log is continually updated and transmitted not just to Ruangguru, via the domain **tracker.ruangguru.com**, but also to Facebook via the **domain graph.facebook.com**.

Ruangguru may surveil its virtual classrooms to target children with behavioral advertising. Ruangguru discloses in its privacy policy that it "may collect interaction information on the page (such as scrolling, clicks, or mouse movement)," for which "we'll use this information … to measure and understand the effectiveness of the advertising we do to you and other parties, and to serve advertisements for products and services that are relevant to you."[148] Ruangguru also notes that it may share this intimate information with "[a]dvertisers and ad networks that require data to select and offer relevant advertisements to you and other users," and that "[w]e may use the personal data we collect to fulfill advertisers' requests by showing their ads to that target audience," though it does not disclose the identity of the advertisers and third-party companies that receive children's data.

However, Ruangguru misleadingly states that it does "not disclose information about identifiable individuals, but we may provide them with aggregated information about our users."[149] However, forensic testing proves otherwise. Human Rights Watch and the Defensive Lab Agency found Ruangguru transmitting its students' Android Advertising ID to AppsFlyer and to Facebook.

Ruangguru also tags its students' devices with an additional, proprietary identifier and sends it back to itself through the domains **gw.ruangguru.com** and **tracker.ruangguru.com**. t appears that the company directly engages in user profiling itself. Its privacy policy discloses that Ruangguru collects even more information about its students from other sources and combines it with the data it holds about its students for advertising and other purposes.[150]

Ruangguru did not respond to our request for comment. In its response, Meta did not address whether Meta was receiving user data from Ruangguru. AppsFlyer responded that the company does not sell or serve any ads, build targeting profiles, or sell data, and did not specifically address our questions about Ruangguru.[151]

Case study: MUSE, Pakistan

Recommended by Pakistan's Ministry of Federal Education and Vocational Training, MUSE is an app built by SABAQ Learning Systems, a Pakistani "award-winning EdTech company."[152] MUSE is targeted at students from kindergarten to fifth grade, and offers "content made for young learners: fun video lessons with lovable animated characters that keep students engaged."[153] In April 2020, The News reported that almost 120,000 students were using MUSE in over 1,000 schools, and that the federal government was working on disseminating the app to the country's lower primary school students.[154] In June 2020, MUSE reported user growth by 200 percent after school closures began.[155]

Forensic analysis found that MUSE collects and transmits its students' personal data to two companies—Facebook and Google—through the six SDKs embedded in the app.

When a child opens up MUSE on their phone, Facebook's embedded SDKs immediately

148 Ruangguru, "Privacy Policy" ("Kebijakan Privasi"), https://web.archive.org/web/20210623100922/https://www.ruangguru.com/privacy-policy (accessed August 4, 2021).

149 Ibid.

150 Ibid. "We may combine information we receive from other sources with information you provide and information we collect. We may use this information as well as the combined information for the purposes set out above."

151 Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; and with Danielle Blumenstyk Peterman, Head of Corporate Comms, AppsFlyer, April 6, 2022.

152 Government of Pakistan, Ministry of Federal Education and Professional Training, "COVID Projects," https://web.archive.org/web/20210804231133/http://www.mofept.gov.pk/Detail/YWUyZTdlM2QtNjQ1ZS00MTJlLWIwYjktYjkoN2E3NmU3YmNj (accessed August 4, 2021); Muse, "About Us: Curiosity is Natural," https://web.archive.org/web/20200711124907/http://muse-lessons.com/Home/About (accessed August 4, 2021); Arshad Yousafzai, "Donated lessons help put Teleschool on air within two weeks," The News, April 27, 2020, https://www.thenews.com.pk/print/650286-donated-lessons-help-put-teleschool-on-air-within-two-weeks (accessed August 4, 2021).

153 Muse, "Product: Seriously Fun," https://web.archive.org/web/20200715123323/http://muse-lessons.com/Home/Product (accessed July 15, 2021); e-Taleem, one portal for digital education, "Current e-learning vertices," https://web.archive.org/web/20210805220937/https://etaleem.gov.pk/ (accessed August 4, 2021).

154 Sumera Naqvi, "Is e-learning the inevitable future?" The News, April 2020, https://web.archive.org/web/20200421043621/https://www.thenews.com.pk/magazine/you/647186-is-e-learning-the-inevitable-future (accessed August 5, 2021).

155 Mehreen Zahra-Malik, "The coronavirus effect on Pakistan's digital divide," *BBC Worklife*, July 13, 2020, https://www.bbc.com/worklife/article/20200713-the-coronavirus-effect-on-pakistans-digital-divide (accessed August 4, 2021).

begin to track their every movement and activity in MUSE's virtual classrooms. This log is continually updated and transmitted to Facebook's domain **graph.facebook.com**. These data are further bundled and sent together with the child's Android Advertising ID, Android ID, information about the device they use, and other personal data, allowing Facebook to tie all of this information together with the child's AAID to build detailed profiles of each child.

MUSE transmits children's data to Facebook even before the child has opened the app for the first time; the app sends this data regardless of whether the child is logged into their Facebook account, or even has a Facebook account at all. Forensic testing revealed that MUSE notifies Facebook the instant the app is installed on the child's device; the app also finds and sends the child's AAID and other information about the child's device in the same data package to **graph.facebook.com**. By tagging and sending the child's persistent identifier to Facebook, MUSE sets the stage for the future collection and transmissions of that child's personal data to be tied to the user profile that Facebook keeps on them, which in turn can be used to target that child with behavioral advertising over time.

Similarly, MUSE transmits the child's AAID and other information about the child's device to Google through the domains **app-measurement.com** and **play.googleapis.com**.

All combined, the app sends more data about children to Facebook and to Google than it sends to itself. Human Rights Watch found that MUSE's data practices are unnecessary and disproportionate to the purpose of providing its child users with learning.

MUSE's privacy policy discloses that the app "may collect … the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile internet browser you use, unique device identifiers and other diagnostic data."[156] However, it does not disclose the data practices observed by Human Rights Watch.

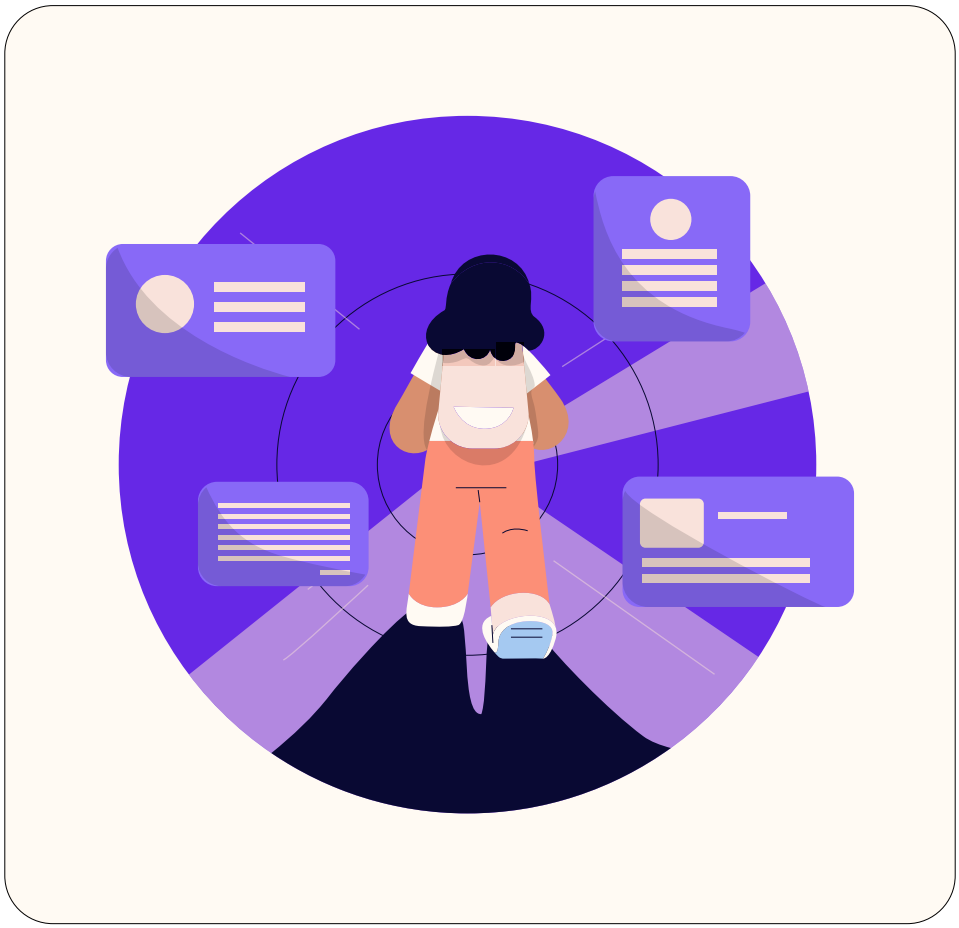
When contacted for comment, MUSE stated that it did not believe that it has "collected children specific data from the app," and doesn't maintain "any repository of children's data." MUSE also confirmed that the app included "data sharing SDKs."[157] In later correspondence, MUSE also stated that "the data is collected of the user so we can better understand what content items were viewed more than others," and that "Google and Facebook SDKs collect this data without sharing any data about a specific user – rather it collects the data of each user as a data point to understand overall usage."

In its response to Human Rights Watch, Meta (Facebook) did not address whether it was receiving children's user data from MUSE.[158] Google did not respond to our request for comment.

156 SABAQ, "MUSE Privacy Policy," June 22, 2019, https://web.archive.org/web/20210223231856/http://sabaq.edu.pk/MusePrivacyPolicy/ (accessed August 4, 2021).

157 Human Rights Watch email correspondence with Hassan Bin Rizwan, Founder, SABAQ / MUSE, April 2, 2022.

158 Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022.



Tracking Children Outside of the Classroom

My teacher makes me download Facebook, BiP, and WhatsApp for school. I don't like these apps, because they understand and see everything that I do. They read my messages. They see everything that I do on my phone. This makes me feel bad.

—Rodin R., a nine-year old student in Istanbul, Turkey[159]

Many children are tracked and surveilled even after they leave the virtual classroom. Human Rights Watch identified companies that track children online, outside of school hours, deep into their private lives, and over time.

159 Human Rights Watch interview with Rodin R., 9, Istanbul, Turkey, June 11, 2021.

Websites: Cookies

A cookie is a small piece of data that companies store in a person's web browser in order to uniquely identify that person. While not all cookies are trackers, third-party cookies are generally used by advertising and tracking companies to watch what people do online, infer their characteristics and interests, and deliver customized ads that then follow them around the internet.

Human Rights Watch found that children's educational websites inserted as many third-party cookies on personal devices as do the world's most popular websites aimed at adults. Out of a total 125 EdTech websites, Human Rights Watch detected 67 EdTech websites that had a total of 472 third-party cookies embedded in them. A child logging into a single one of these 67 platforms might be tracked on average by seven cookies or encounter a median of three cookies. Meanwhile, an investigation conducted by The Markup in September 2020 found that of the world's over 80,000 most popular websites, a list that includes global e-commerce giants that deploy extensive advertising, a site loaded a median of three third-party cookies.[160]

Put another way, children are surveilled in their virtual classrooms and followed long after they leave, outside of school hours and across the internet, at a similar rate as adults shopping in the world's largest virtual malls.

The number of AdTech or other third-party companies receiving children's data was discovered to be even greater than the number of EdTech sites sending this data to them. Human Rights Watch detected 67 websites transmitting children's data to 85 AdTech or third-party companies.

Some EdTech sites installed dozens of cookies. Human Rights Watch found 76 cookies installed on Z-kai, recommended by the Japanese government and noted earlier in this chapter as having installed the highest number of ad trackers amongst the EdTech websites analyzed by Human Rights Watch. These cookies trailed students even after they left Z-kai's website to go elsewhere on the web, sending their whereabouts and activities to 31 AdTech companies.

Case study: 100Ballov, Kazakhstan

Some EdTech sites chose to install cookies by AdTech companies that engage in particularly deceptive practices. On April 3, 2020, children in Kazakhstan began logging into their first day of online classes, in accordance with their government's pivot to online learning. Many of these children opened up 100Ballov, endorsed by the Education Ministry and adopted by schools as the "educational portal for schoolchildren and students."[161]

Human Rights Watch detected 100Ballov sending information about its students to AddThis, a marketing company acquired by Oracle in 2016.[162] AddThis offers a set of social media share buttons that allows website users to easily share interesting content on social media.

160 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/black-light/2020/09/22/how-we-built-a-real-time-privacy-inspector#survey (accessed July 12, 2021); Victor Le Pochat et al., "Tranco," generated on July 13, 2021, https://tranco-list.eu/list/KLPW/1000000 (accessed July 13, 2021); see also, Victor Le Pochat et al., "TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

161 Electronic Government of the Republic of Kazakhstan, e-gov, "Spheres," https://web.archive.org/web/20210901181204/https://egov.kz/cms/en/covid/spheres (accessed September 1, 2021); City of Pavlodar Education Department, "Online Testing" ("ТЕСТИРОВАНИЕ ON-LINE"), https://web.archive.org/web/20210901213326/https://goo.edu.kz/content/view/30/20228?lang=-ru (accessed September 1, 2021); see also example of a school; School Gymnasium No 28, "Dear Teachers and Parents!" ("Құрметті ұстаздар мен ата-аналар!"), March 27, 2020, https://web.archive.org/web/20210121140648/https://kst28mg.kz/2020/03/27/%D2%9A%D2%B1%D1%80%D0%BC%D0%B5%D1%82%D1%82%D1%96-%D2%B1%D1%81%D1%82%D0%B0%D0%B7%D0%B4%D0%B0%D1%80-%D0%BC%D0%B5%D0%BD%D0%B0%D1%82%D0%B0-%D0%B0%D0%BB%D0%B0%D0%B0%D1%80/ (accessed September 1, 2021).

162 Oracle, "Oracle buys AddThis," January 5, 2016, https://www.oracle.com/corporate/acquisitions/addthis/ (accessed September 1, 2021).

But AddThis does much more than encourage social media traffic. Whether or not a person clicks on the "share" button, AddThis instantly loads dozens of cookies and tracking pixels on website visitors' browsers, like nesting dolls, each collecting and sending user data to Oracle and to dozens of other AdTech companies to profile and target a person or a child with behavioral advertising that follows them across the internet.[163]

AddThis' privacy policy states:

> The AddThis Tools also incorporate Cookies and Pixels from Oracle partners to enable the synchronization of unique identifiers between Oracle and our third-party partners to facilitate online behavioral advertising across the online advertising ecosystem.[164]

Human Rights Watch found six AddThis cookies on 100Ballov, which in turn loaded four other trackers by AddThis' advertising partners: two cookies pointing to DoubleClick, Google's advertising division, and two to Tapad.[165] Tapad, an AdTech company, describes its services as "enabl[ing] marketers to identify a brand customer or related household across multiple devices, unlocking key use cases across programmatic targeting, media measurement, attribution, and personalization globally."[166]

100Ballov did not disclose this practice on its website; it does not have a privacy policy at all.[167] AddThis' button is not visible on any of 100Ballov's webpages, indicating that AddThis and its nested cookies were harvesting children's data without even providing its purported social media functionality, as well as denying children knowledge of these tracking practices.

In response to our request for comment, Oracle stated that any receipt of children's data through its AddThis tools is a violation of Oracle's policies, which prohibit advertising partners and website publishers from sending personal information from sites directed to children under 16 years old, or from consumers these companies know to be under 16 years old.[168] Oracle did not address whether it had received children's data from 100Ballov.

100Ballov did not respond to our request for comment.

163 Aaron Sankin and Surya Mattu, "The High Privacy Cost of a "Free" Website," The Markup, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites (accessed July 12, 2021).

164 AddThis, "Privacy Policy," January 4, 2021, https://web.archive.org/web/20210831042530/https://www.oracle.com/legal/privacy/addthis-privacy-policy.html (accessed August 31, 2021).

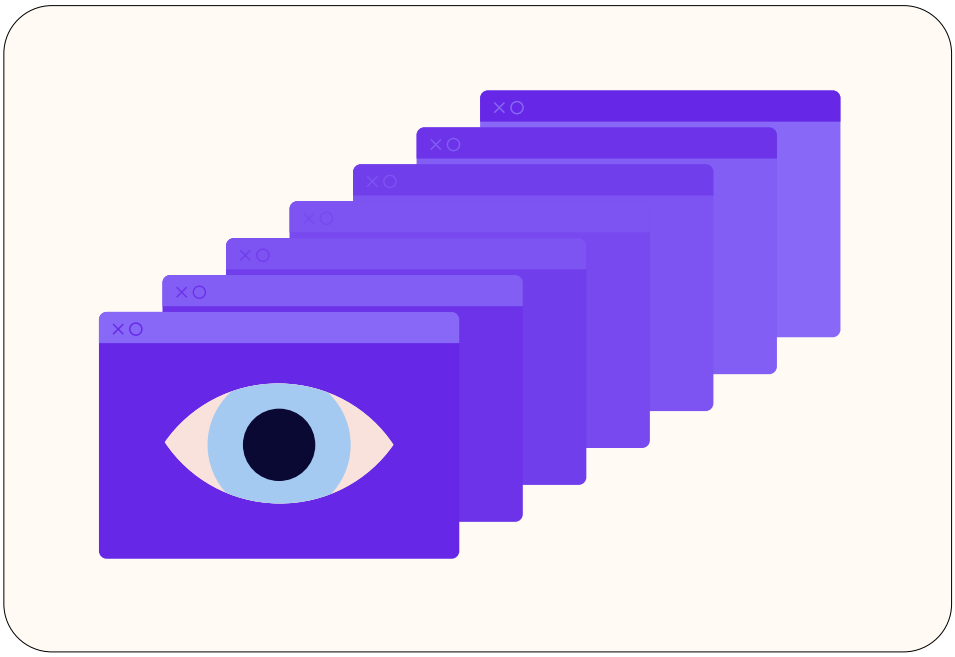
165 AddThis, "Cookie & Pixel Partners," https://web.archive.org/web/20210901224150/https://www.addthis.com/privacy/pixel-partners/ (accessed September 1, 2021).

166 Tapad, "tapad.com," https://web.archive.org/web/20210806200105/https://www.tapad.com/ (accessed August 6, 2021).

167 100Ballov offers a dummy "Privacy Policy" link, which points back to the site's homepage. See: 100Ballov, "100Ballov.kz," https://web.archive.org/web/20210308194123/https://100ballov.kz/ (accessed March 8, 2021).

168 Human Rights Watch correspondence with Dorian Daley, Executive Vice President and General Counsel, Oracle, April 15, 2022; Oracle, "Oracle Advertising Privacy Policy," https://www.oracle.com/legal/privacy/advertising-privacy-policy.html (accessed April 25, 2022); Oracle, "AddThis Privacy Policy," https://www.oracle.com/legal/privacy/addthis-privacy-policy.html (accessed April 25, 2022).

III. Hidden Manipulation: How Children's Data Are Used



These companies, they don't let us know. They're not transparent with us, saying that this is exactly where your data goes, and this is exactly what happens with it. We're trusting them blindly without knowing what's going on. And us kids won't doubt it at all—we won't even think that something bad is happening behind our backs. The amount that we've shared, all that we've done online, that it's all gone to some strange person … The whole idea starts haunting you, and you get really scared.

—Priyanka S., 16, Uttar Pradesh, India[169]

Profiled and Targeted

Most online learning platforms used during the pandemic secretly harvested vast amounts of data from children, piecing them together to deduce each child's characteristics, behaviors, and interests. Combined in this way, personal data can uniquely identify a child; algorithms can mine this data to guess at a child's identity, location, interests, emotions, health, and relationships, and use these inferences to predict what a child might do next, or how they might be influenced.

Profiling and targeting children on the basis of their actual or inferred characteristics not only infringes on their privacy, but also risks abusing or violating their other rights, particularly when this information is used to anticipate and guide them toward outcomes that are harmful or not in their best interest.

169 Human Rights Watch interview with Priyanka S., 16, Uttar Pradesh, India, August 2, 2021.

Such practices also play an enormous role in shaping children's online experiences and determining the information they see, which can influence, shape, or modify children's opinions and thoughts in ways that exploit their lack of understanding, affect their ability to make autonomous choices, and limit their opportunities or development. Such practices may also have adverse consequences that continue to affect children at later stages of their lives.[170]

The United Nations Committee on the Rights of the Child has warned that such processing and use of children's data "may result in violations or abuses of children's rights," and has called on states to "prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling."[171]

The Office of the High Commissioner for Human Rights has stated more broadly that the mass collection and processing of fine-grained information about people's lives to infer their physical and mental characteristics, profile, and make decisions about them "carries risks for individuals and societies that can hardly be overestimated,"[172] with implications for people's access to health care, financial services, and due process rights, among others. In guidelines issued to its member states, the Council of Europe stated: "Profiling of children, which is any form of automated processing of personal data which consists of applying a 'profile' to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law."[173]

Below, we discuss the different ways in which user profiles on children can be misused. Human Rights Watch found that EdTech's profiling and targeting of children did not yield any educational benefit to children; furthermore, the invasiveness of these data practices stands in sharp contrast to the strict limits and laws that governments place on the collection, sharing, and use of student data by schools.

Behavioral Advertising

Children are particularly susceptible to advertising, due to their still-developing cognitive abilities and impulse inhibition. Research on children's cognitive development in relation to television commercials has demonstrated that younger children, particularly those under 7 years old, cannot identify ads or understand their persuasive intent; children at 12 years and older begin to distinguish between organic content and advertisements, though this does not translate into their ability to resist marketing.[174] On the internet, much like adults, many older children and teenagers struggle with understanding the opaque supply chain of commercial activity in which their personal data are valued, traded, and used.[175]

170 Council of Europe, "Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications," DGI (2017)12, March 2018, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (accessed July 15, 2021), p. 15-16.

171 Committee on the Rights of the Child, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 42.

172 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 40; UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/39/29, August 3, 2018, paras. 15, 16.

173 Council of Europe, "Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment," Recommendation CM/Rec (2018)7 of the Committee of Ministers, September 2018, https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html (accessed July 15, 2021), para. 37.

174 Deborah Roedder John, "Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research," Journal of Consumer Research, vol. 26, no. 3 (1999): accessed July 14, 2021, doi: 10.1086/209559; Brian L. Wilcox et al., "Report of the APA Task Force on Advertising And Children," American Psychological Association, February 20, 2004, https://www.apa.org/pi/families/resources/advertising-children.pdf (accessed July 14, 2021).

175 Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, "Children's Data and Privacy Online: Growing Up In a Digital Age. An Evidence Review," London School of Economics and Political Science, January 2019, http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (accessed July 15, 2021), p. 15; Jenny Radesky et al., "American Academy of Pediatrics Policy Statement: Digital Advertising to Children," *Pediatrics*, vol. 146, no. 1 (2020): accessed June 8, 2021, doi: 10.1542/peds.2020-1681.

Children are at even greater risk of manipulation by behavioral advertising online.[176] When children's data are collected for advertising, sophisticated algorithms extract and analyze overwhelming amounts of children's personal data for the purpose of tailoring ads accurately. These ads are embedded in personalized digital platforms that further blur the distinctions between organic and paid content. In doing so, behavioral advertising capitalizes on children's inabilities to identify or critically think about persuasive intent, potentially manipulating them toward outcomes that may not be in their best interest.[177]

Behavioral advertising is even more egregious when targeted at children in settings where they cannot realistically refuse it. In the absence of alternatives, children faced a singular choice whether they were aware of it or not: attend school and use an EdTech product that infringes upon their privacy, or forgo the product altogether, be marked as absent, and be forced to drop out of school during the pandemic. Furthermore, as children spent a considerable amount of their childhood online in virtual classrooms during Covid-19 lockdowns, they were maximally exposed to the risks of collection and exploitation of their personal data.

The Committee on the Rights of the Child has stated that countries "should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling."[178] In a statement issued to pediatric health care providers, industry, and policy makers, the American Academy of Pediatrics raised concerns "about the practice of tracking and using children's digital behavior to inform targeted marketing campaigns, which may contribute to health disparities among vulnerable children or populations."[179]

Human Rights Watch found that 199 third-party companies, most of them AdTech companies, received children's personal data from just 146 EdTech products. Put another way, the number of advertising companies receiving children's data vastly outnumber the number of EdTech companies collecting children's data.

Most EdTech companies concealed their data surveillance practices. Of the total 164 EdTech products reviewed by Human Rights Watch, only 35 disclosed in their privacy policies that their users' data was used for behavioral advertising. Of these, 23 products were developed with children as their primary users in mind, suggesting that behavioral advertising to children was an intended feature of the EdTech product.

176 Livingstone, Stoilova, and Nandagiri, "Children's Data and Privacy Online: Growing Up In a Digital Age, An Evidence Review," p. 15; Radesky et al., "American Academy of Pediatrics Policy Statement: Digital Advertising to Children."; Eva A. van Reijmersdal et al., "Processes and effects of targeted online advertising among children," *International Journal of Advertising*, vol. 36, no. 3 (2017):, pp. 396-414, accessed July 15, 2021, doi: 10.1080/02650487.2016.1196904.

177 One study of 231 Dutch children aged 9-13 years found that children process behavioral advertising in fundamentally different ways than adults do. Children processed behavioral ads non-critically, and did not seem to understand the targeting tactic or think that profile-targeted ads were more relevant to them. At the same time, seeing behavioral ads that were targeted at their interests and hobbies proved to be effective in creating positive associations toward the brand and increased children's intention to buy the products. See: van Reijmersdal et al., "Processes and effects of targeted online advertising among children," pp. 396-414.

178 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 42.

179 Radesky et al., "American Academy of Pediatrics Policy Statement: Digital Advertising to Children."

Case Study: ȘcoalaIntuitext, Romania

Recommended by Romania's Education Ministry, ȘcoalaIntuitext discloses in its privacy policy that it installs 23 marketing cookies in order to target its students with behavioral advertising across the internet.

Excerpt from ȘcoalaIntuitext's Privacy Policy, as seen on May 2, 2022.[180]

> Marketing cookies are used to track users from one site to another. The intent is to show relevant and engaging ads to individual users, so they are more valuable to advertising agencies and third parties dealing with advertising.

Name	Provider	Purpose	Expiry	Type
_ _zlcmid	Zendesk	Preserves users states across page requests.	1 year	HTTP cookie
_fbp	Meta Platforms, Inc.	Used by Facebook to deliver a series of advertising products such as real time bidding from third party advertisers.	3 months	HTTP cookie
_gcl_au	Google	Used by Google AdSense for experimenting with advertisement efficiency across websites using their services.	3 months	HTTP cookie
_hjRecording-Enabled	Hotjar	This cookie is used to identify the visitor and optimize ad-relevance by collecting visitor data from multiple websites – this exchange of visitor data is normally provided by a third-party data-center or ad-exchange.	Session	HTML Local Storage
ads/ ga-audiences	Google	Used by Google AdWords to re-engage visitors that are likely to convert to customers based on the visitor's online behaviour across websites.	Session	Pixel Tracker
fr	Meta Platforms, Inc.	Used by Facebook to deliver a series of advertisement products such as real time bidding from third party advertisers.	3 months	HTTP Cookie
IDE	Google	Used by Google DoubleClick to register and report the website user's actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.	1 year	HTTP Cookie

When contacted for comment, Softwin, the Romanian EdTech company that operates ȘcoalaIntuitext, said that the product is "actually dedicated first to teachers/educators and only in a subsidiary way to children or their parents." The company acknowledged that it sends user data through marketing cookies, Facebook Pixel, and Google Analytics' 'remarketing audiences' feature, and that it does so to target adults "in the places where our main customers (teachers/educators) are active," including on Facebook and on Google. Softwin responded that, "To be clear no children's data collected by ScoalaIntuitext.ro is used for advertising, behavioral advertising, or any other commercial purposes."

180 The first seven of the 23 marketing cookies listed in the privacy policy are excerpted here as examples. For the full list, see: ȘcoalaIntuitext, "Personal Data Processing Policy" ("Politica De Prelucrare Date Personale"), May 18, 2018, https://web.archive.org/web/20220502221207/https://www.scoalaintuitext.ro/politica-de-confidentialitate; https://www.scoalaintuitext.ro/politica-de-confidentialitate (accessed May 2, 2022).

It denied that it sends children's data to third parties or AdTech companies and said that the children's data it collects is not used for advertising, behavioral advertising, or user profiling.[181]

However, ȘcoalaIntuitext is marketed for children's use. Its home page features a marketing message directed at students that explains the benefits of the product.[182] Another page on the website, titled "Children," is directed to would-be child users and states that, "ȘcoalaIntuitext is an educational platform … intended for primary school students (Preparatory classes – IV), their parents and primary school teachers."[183]

The page also asks students to advertise ȘcoalaIntuitext to their teacher: "Share with your teacher that you have discovered this useful application and enjoy the benefits of ȘcoalaIntuitext TOGETHER," and features four share buttons which, when clicked, opens a social media platform or new email message and prompts the student user to log in to share pre-populated text inviting the recipient, presumably their teacher, to use ȘcoalaIntuitext.[184]

Human Rights Watch found that ȘcoalaIntuitext embedded tracking technologies on pages that were likely to be accessed by children, including the page titled "Children," and observed ȘcoalaIntuitext sending user data to AdTech companies through the third-party marketing cookies, Facebook Pixel and Google Analytics' 'remarketing audiences' feature that it acknowledged. The company did not acknowledge its use of ad trackers and session recording.[185] Human Rights Watch did not find evidence that these data practices were limited to adults.

181 Human Rights Watch email correspondence with Alexandru Neagu, Legal Advisor, Softwin, April 8, 2022.

182 ȘcoalaIntuitext, "Școala Intuitext," https://web.archive.org/web/20220502210616/https://www.scoalaintuitext.ro/ (accessed May 2, 2022).

183 ȘcoalaIntuitext, "Copii" ("Children"), https://web.archive.org/web/20220502213856/https://www.scoalaintuitext.ro/copii (accessed May 2, 2022).

184 Ibid.

185 Human Rights Watch email correspondence with Alexandru Neagu, Legal Advisor, Softwin, April 8, 2022.

Human Rights Watch also found that five governments directly built and offered EdTech products for which they disclosed, through their privacy policies, that they use children's personal data to target behavioral advertising back at them.

Country	EdTech Product	Privacy Policy
Canada	CBC Kids	"The data collected when you visit our website or click on our digital ads is used to show you future ads that match your interests. Ad targeting is used to create larger group profiles and larger audience segments made of users across Canada that share common interests." "Our advertising partners use cookies to show you ads. They'll look at the cookies you already have on your browser and decide whether and which ad they want to place on our site for you to see."[186]
Ghana	Ghana Library Mobile Application	"We may use information collected about you via the Application to … Deliver targeted advertising, coupons, newsletters, and other information regarding promotions and the Application to you" and "Offer new products, services, mobile applications, and/or recommendations to you." "We may share your information with third parties for marketing purposes … Additionally, we may use third-party software to serve ads on the application, implement email marketing campaigns, and manage other interactive marketing initiatives. This third-party software may use cookies or similar tracking technology to help manage and optimize your online experience with us."[187]
Indonesia	Rumah Belajar	"We may share Your information with Our business partners to offer You certain products, services or promotions." "We may share Your personal information with Service Providers to … show advertisements to You to help support and maintain Our Service, to contact You, to advertise on third party websites to You after You visited our Service." "The information gathered via these Cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the Website. We may also use these Cookies to test new advertisements … to see how our users react to them."[188]
Republic of Korea	EBS	"‹Korea Education Broadcasting Corporation› processes personal information for the following purposes: Use for marketing and advertising. Personal information is processed for the purpose of developing new services (products) and providing customized services, providing event and advertising information." "The company uses cookies for the following purpose: to provide targeted marketing and personalized services by analyzing the frequency and time of visits by members and non-members, identifying, tracing, and tracking users' preferences and interests, and identifying the degree of participation in various events and the number of visits, etc."[189]

186 Canadian Broadcasting Corporation, "CBC and your data," March 30, 2020, https://web.archive.org/web/20210806100359/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726 (accessed August 6, 2021).

187 Ghana Library Authority, "Ghana Library App Privacy Policy," June 5, 2020, https://web.archive.org/web/20210303152004/http://142.11.195.10/digital_library/privacy_policy.html (accessed August 6, 2021).

188 Rumah Belajar, "Privacy Policy," February 4, 2020, https://web.archive.org/web/20210807042148/http://apps.belajar.kemdikbud.go.id/privacypolicy.html (accessed August 6, 2021).

189 EBS, "Privacy Policy" ("개인정보처리방침"), February 8, 2021, https://web.archive.org/web/20210804035422/https://sso.ebs.co.kr/policy/privacy?date=20210208&tab=2&ver=%2Fpolicy%2Fprivacy%3Fdate%3D20210208&fsdc= (accessed August 6, 2021), art. 1 (다), art. 8 (가).

South Africa	Ministry of Education's website	"National Department of Basic Education also uses your personally identifiable information to inform you of other products or services available from National Department of Basic Education and its affiliates." "National Department of Basic Education may, from time to time, contact you on behalf of external business partners about a particular offering that may be of interest to you." "National Department of Basic Education keeps track of the Web sites and pages our customers visit within National Department of Basic Education … This data is used to deliver customized content and advertising within National Department of Basic Education to customers whose behavior indicates that they are interested in a particular subject area."[190]

Case Study: CBC Kids, Canada

When a child opens CBC Kids, offered by the Canadian Broadcasting Corporation and recommended by Canada's Quebec Education Ministry for pre-primary and primary school-aged children's learning, the first thing they see on the page are large, brightly colored tiles.[191] In July 2021, the first tile featured a photo marked by a heart emoji and captioned, "AWW: Check out these cute baby animals." Another tile was filled with brightly colored characters and titled "MONSTER MATH! Are you a math wizard? Let's find out." The front page also offered the newest episode of "The Adventures of Paddington;" the link was decorated with the smiling face of the famous fictional bear, waving his paw at the viewer.

Screenshot of the CBC Kids website, as viewed by Human Rights Watch in July 2021. © CBC Kids

190 Government of South Africa, National Department of Basic Education, "Privacy Statement," https://web.archive.org/web/20210807041929/https://www.education.gov.za/privacy.aspx (accessed August 4, 2021).

191 CBC Kids, "CBC Kids," https://web.archive.org/web/20210720010630/https://www.cbc.ca/kids/ (accessed July 20, 2021). See also: Government of Quebec ("Gouvernement du Québec"), Ecole Ouverte, "CBC Kids," June 15, 2021, https://ecoleouverte.ca/notice?id=p%3A%3Ausmarcdef_0000039521&queryId=4ddadb89-795b-45bf-a8fc-ee66084ba836&posInSet=1 (accessed July 12, 2021).

At the same time, when the child opens up the website, an invisible swarm of ad trackers and cookies get to work. Human Rights Watch found 29 third-party trackers collecting and sending data about children to 18 companies, mostly AdTech, and another 15 third-party cookies sending children's data to nine companies, mostly AdTech. To put this into perspective, this is more than five times the median number of three cookies and more than four times the median of seven ad trackers installed on the world's most popular internet sites—sites that include heavily trafficked e-commerce sites with explicit business interests in marketing.[192]

15 third-party cookies on CBC Kids collected and sent children's data to 9 companies

AdTech company	Receiving domains
Adobe	demdex.net, dpm.demdex.net
Bombora	ml314.com
Google	doubleclick.net
LiveRamp	rlcdn.com, rlcdn.com
Lotame	crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net, crwdcntrl.net
Neustar	agkn.com
Piano	cxense.com
The Trade Desk	adsrvr.org
WarnerMedia	adnxs.com

29 ad trackers on CBC Kids collected and sent children's data to 18 companies

AdTech company	Receiving domains
Adobe	adobedtm.com, demdex.net, everesttech.net, omtrdc.net
Akamai Technologies	akstat.io, edgekey.net, go-mpulse.net
Amplitude	amplitude.com
Bombora	ml314.com
Chartbeat	chartbeat.com, chartbeat.net
Cheetah Digital (formerly Wayin)	wayin.com
comScore	scorecardresearch.com
Conductrics	conductrics.com
Facebook	facebook.com, facebook.net
Google	google-analytics.com, googlesyndication.com, googletagmanager.com, googletagservices.com, doubleclick.net
LiveRamp	rlcdn.com
Lotame	crwdcntrl.net
Neustar	agkn.com
Oracle	bluekai.com
Piano	cxense.com
Skimbit	skimresources.com
The Nielsen Company	exelator.com
Throtle	thrtle.com

192 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector#survey (accessed July 12, 2021); Victor Le Pochat et al., "Tranco," generated on July 13, 2021, https://tranco-list.eu/list/KLPW/1000000 (accessed July 13, 2021); see also, Victor Le Pochat et al., "TRANCO: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), accessed July 13, 2021, doi:10.14722/ndss.2019.23386.

Altogether, 20 companies involved in advertising and marketing received data about children from CBC Kids. Of these, six AdTech companies receiving data from CBC Kids—Adobe, Facebook, Google, LiveRamp, Piano, The Trade Desk—offer services to match website visitors to personally identifiable information sourced from other online and offline records, including physical addresses, location data, and credit scores,[193] building or enhancing a comprehensive profile about that person that can be used and sold to "serve targeted advertising and content to the right audience" (Adobe)[194] or to "understand and influence customer behavior" (Piano).[195]

Of the 20 companies, seven companies—comScore, LiveRamp, Lotame, Neustar, Oracle, The Nielsen Company, and Throtle—have formally registered themselves with the California Data Broker Registry as data brokers, that is, companies whose primary business is the packaging and selling of people's personal data.[196]

Lotame, for instance, bills itself as the "World's Largest 2nd and 3rd Party Data Marketplace" and "supplies real-time access to a firehose of raw behavioral data from billions of consumer profiles" which can be used to create user profiles.[197] The company assures advertisers that they "can add demographic, behavioral, geographic, and other types of data to learn more about your customers and find new ways to monetize those audiences."[198] Human Rights Watch detected CBC Kids sending children's data to Lotame through five cookies and an ad tracker.

193 The Trade Desk shares and sells personal data from third-party data brokers such as Experian and Equifax, two credit scoring companies, and PlaceIQ, Acxiom, and Foursquare, which provide location data. See: The Trade Desk, "Our Partners," https://web.archive.org/web/20210720042303/https://www.thetradedesk.com/us/our-platform/our-partners (accessed July 19, 2021).

194 Adobe Experience League, "Audience Manager Overview," last updated April 13, 2021, https://web.archive.org/web/20210807045536/https://experienceleague.adobe.com/docs/audience-manager/user-guide/overview/aam-overview.html?lang=en (accessed July 19, 2021).

195 Piano.io, "Piano," https://web.archive.org/web/20210807045609/https://piano.io/ (accessed July 19, 2021.

196 The US State of California defines a data broker as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship," and notes that: "A data broker collects many hundreds or thousands of data points about consumers from multiple sources … then analyzes the data to assess content and packages the data for sale to a third party," and that data brokers "create risks that are associated with the widespread aggregation and sale of data about consumers, including risks related to the inability of consumers to know and control information held and sold about them and risks arising from the unauthorized or harmful acquisition and use of consumer information." See: AB-1202 Privacy: data brokers, Assembly Bill No. 1202, Chapter 753, October 11, 2019, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202 (accessed July 19, 2021), section 2 (d), section 1 (d), (f), (h). To see these companies' self-declarations, see the following submissions in the California Data Broker Registry: US State of California Department of Justice, "Data Broker Registration for Comscore, Inc.," January 30, 2020, https://web.archive.org/web/20210720003259/https://oag.ca.gov/data-broker/registration/186289 (accessed July 19, 2021); US State of California Department of Justice, "Data Broker Registration for LiveRamp, Inc.," March 19, 2020, https://web.archive.org/web/20220223115800/https://oag.ca.gov/data-broker/registration/188120 (accessed May 2, 2021); US State of California Department of Justice, "Data Broker Registration for Lotame Solutions, Inc.," February 27, 2020, https://web.archive.org/web/20210720003420/https://oag.ca.gov/data-broker/registration/186954 (accessed July 19, 2021); US State of California Department of Justice, "Data Broker Registration for Neustar, Inc.," March 23, 2020, https://web.archive.org/web/20210720003647/https://oag.ca.gov/data-broker/registration/186862 (accessed May 2, 2021); US State of California Department of Justice, "Data Broker Registration for Oracle America, Inc., Oracle Data Cloud" March 11, 2020, https://web.archive.org/web/20210720003817/https://oag.ca.gov/data-broker/registration/185679; (accessed July 19, 2021); US State of California Department of Justice, "Data Broker Registration for Nielsen Marketing Cloud," August 11, 2020, https://web.archive.org/web/20210720004748/https://oag.ca.gov/data-broker/registration/187679 (accessed July 19, 2021); US State of California Department of Justice, "Data Broker Registration for Throtle," January 31, 2020, https://web.archive.org/web/20210720003927/https://oag.ca.gov/data-broker/registration/185964, (accessed July 19, 2021).

197 Lotame, "Lotame Data Exchange," https://web.archive.org/web/20210720045203/https://www.lotame.com/products/lotame-data-exchange/ (accessed July 19, 2021); Lotame, "Data Stream," https://web.archive.org/web/20210807045456/https://www.lotame.com/products/lotame-connect/data-stream/ (accessed July 19, 2021).

198 Lotame, "How Identity Graphs Benefit a Connected Digital Advertising Ecosystem," December 11, 2020, https://web.archive.org/web/20210720050850/https://www.lotame.com/how-identity-graphs-benefit-a-connected-digital-advertising-ecosystem/ (accessed July 19, 2021).

Human Rights Watch also found CBC Kids sending data about children to The Nielsen Company, which claims that it can "understand the personality of your customers and prospects to effectively forecast behavior with the largest personality database in the world."[199] Specifically, Human Rights Watch observed CBC Kids transmitting kids' data through the ad tracker exelator.com, which then feeds into the eXelate data pool, "Nielsen's proprietary and highly curated mix of offline and online data," which Nielsen can sell to other companies to "help [them] win the battle for consumer attention."[200]

CBC Kids is covered by the privacy policy of its parent site, CBC, which reassures users that, "The vast majority of the information you create doesn't have any indicator of who you are, personally."[201] However, Human Rights Watch observed CBC Kids sending children's data to companies that claim to connect real people's offline identity records to their online activities.[202] One such company, LiveRamp, claims to "deterministically merg[e] offline PII (personally identifiable information, such as email address, name, postal address, and phone number) and matching to cookies, mobile device IDs, and proprietary platform IDs," into what the company calls RampID.[203] The company draws upon "a multi-billion record set" that includes public record data, publicly available data, and self-reported information.[204]

LiveRamp promises its clients "real-time people-based insights … and build a mapping over time," once clients place the company's Real-Time Identity Service pixel and cookie on their website or advertisement.[205] The pixel is programmed to send user information to LiveRamp's domain **rlcdn.com**.[206]

Human Rights Watch found CBC Kids sending data about the children visiting its website to LiveRamp through two embedded cookies and an ad tracker pointing to the domain **rlcdn.com**, none of which were disclosed in CBC's privacy policy or cookie policy.[207]

CBC discloses in its privacy policy that it engages in user profiling and behavioral advertising (see table above), but does not disclose the identity of these companies and data brokers that receive children's data, or explain how they might use it. On a child-friendly webpage titled "How to Manage Your Cookies," CBC Kids discloses that it uses "strictly necessary cookies … needed for CBC Kids to work," "functionality cookies … needed for specific features of CBC Kids to work," and "performance cookies [that] help us understand how well the CBC Kids sites are working."[208] However, CBC Kids does not disclose the presence of marketing cookies or ad trackers on its site, or that such tracking technologies are used to send children's data to AdTech companies and data brokers. Moreover, children who accessed this webpage to learn how to opt out of being tracked by cookies were in turn surveilled, and their personal data transmitted, to six AdTech companies. Human Rights Watch detected cookies and ad trackers embedded in the "How to Manage Your Cookies" webpage sending children's data to Adobe, ChartBeat, comScore, Cxense, Google, and Oracle.

199 The Nielsen Company, "Nielsen Data As A Service," https://web.archive.org/web/20210712213654/https://www.nielsen.com/eu/en/solutions/capabilities/nielsenmarketingcloud-daas/ (accessed July 12, 2021); The Nielsen Company, "Nielsen Acquires eXelate," March 4, 2015, https://web.archive.org/web/20210807045818/https://www.nielsen.com/us/en/press-releases/2015/nielsen-acquires-exelate/ (accessed August 7, 2021).

200 Ibid.

201 Canadian Broadcasting Corporation, "CBC and your data," March 30, 2020, https://web.archive.org/web/20210720002724/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726 (accessed July 19, 2021).

202 Neustar, for instance, began as a division within the US defense contractor Lockheed Martin and sells access to its records on over 260 million people, linked to real names, addresses, phone numbers, email addresses, "psychological variables," and "hundreds of demographic, behavioral, financial, property, segmentation and geographic attributes." See: Neustar, "Engage the Right Target Audiences at Scale And Across Channels," https://web.archive.org/web/20210720043836/https://www.home.neustar/adadvisor (accessed July 19, 2021); Neustar, "Customer Identity File," 2020, https://web.archive.org/web/20210904001854/https://www.cdn.neustar/resources/product-literature/marketing/neustar-marketing-customer-identity-file-solution-sheet.pdf (accessed September 3, 2021); Neustar, "Neustar AdAdvisor Reference Guide," 2020, https://web.archive.org/web/20210720044010/https://www.cdn.neustar/resources/product-literature/marketing/neustar-adadvisor-reference-guide.pdf (accessed July 19, 2021), p. 5.

203 LiveRamp, "Identity and Identifier Terms and Concepts: More Information About RampIDs," last modified September 13, 2021, https://web.archive.org/web/20220503064631/https://docs.liveramp.com/safe-haven/en/identity-and-identifier-terms-and-concepts.html (accessed May 2, 2022).

204 Ibid.

205 LiveRamp, "Interpreting RampID, LiveRamp's People-Based Identifier: Delivery Options and Formats," last modified February 23, 2022, https://web.archive.org/web/20220429143904/https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html (accessed May 2, 2022).

206 Ibid. See also: LiveRamp, "Announcing Required Pixel Changes (7/2/2019)," last modified September 9, 2020, https://web.archive.org/web/20211024132941/https://docs.liveramp.com/connect/en/announcing-required-pixel-changes--7-2-19-.html (accessed May 2, 2022).

207 For CBC's privacy policies, see: Canadian Broadcasting Corporation, "View Your Cookies," https://web.archive.org/web/20210720014616/https://www.cbc.ca/mycbc/viewcookies (accessed July 19, 2021); Canadian Broadcasting Corporation, "CBC and your data," March 30, 2020, https://web.archive.org/web/20210720002724/https://www.cbc.ca/mycbc/cbc-and-your-data-1.5514726 (accessed July 19, 2021).

208 CBC Kids, "How to Manage Your Cookies," https://web.archive.org/web/20210627035123/https://www.cbc.ca/kids/about/cookies (accessed June 27, 2021).

When reached for comment, CBC said that it "explicitly prohibit[s] targeting on both our traditional and online platforms" and that "[t]he CBC.ca/kids [CBC Kids] section is ad free."[209] CBC confirmed the presence of 13 trackers on CBC Kids, of which 8 trackers—Adobe, Akamai, Amplitude, Chartbeat, comScore, Conductrics, Piano, Wayin—were used for site performance, functionality, and safety. The company said that another 4 trackers – Lotame, Oracle, Facebook, and Neustar—were inactive, and that trackers from Google were primarily restricted to product performance, though CBC had discovered a Google cookie that it planned to check.[210]

As noted in the methodology of this report, Human Rights Watch conducted the primary phase of its investigation between May and August 2021, and conducted further checks in November 2021 to verify its findings. Human Rights Watch captured evidence, in real time, of CBC Kids transmitting data through the 29 ad trackers and 15 third-party cookies embedded on the site and listed in the tables above. These included the trackers that CBC acknowledged were present but inactive on the site.

While Human Rights Watch could not corroborate CBC's statement that 8 trackers were used to enable core site functionality, other trackers were found sending data to domains explicitly owned by AdTech companies and used for their advertising businesses, including Google's **doubleclick.net**.

When reached for comment, Akamai Technologies did not answer our questions regarding CBC Kids.[211] Adobe, Cheetah Digital, Meta, and Oracle did not acknowledge that they receive data from CBC Kids, and said that it was their customers' responsibility to comply with their policies and applicable laws that prohibit the collection of children's data.[212] LiveRamp said that it was not aware of a contractual or other relationship between LiveRamp and CBC Kids, and requested additional details.[213] LiveRamp had not replied to Human Rights Watch's April 13, 2022 correspondence sharing further technical evidence at the time of this writing.[214]

Bombora denied that it receives data from CBC Kids, but acknowledged that it receives data from CBC's parent site, cbc.ca.[215] However, Human Rights Watch notes that its investigation focused on analyzing the data that was sent from eleven web pages from the CBC Kids domain (cbc.ca/kids).

In a statement, Piano said that it provided services to CBC Kids for the optimization of CBC Kids' search engine, which did not involve the collection of children's data from CBC Kids.[216]

Amplitude did not respond to our questions on CBC Kids. comScore, Google, Lotame, Neustar, and Throtle did not respond to a request for comment.

209 Human Rights Watch email correspondence with Catherine Tait, President and CEO, CBC/Radio-Canada, April 25, 2022.

210 Ibid.

211 Human Rights Watch email correspondence with Gina Sorice, Akamai Technologies, March 22, 2022.

212 Human Rights Watch email correspondence with Adobe, April 8, 2022; with Jill Knesek, Chief Security Officer and Chief Privacy Officer, Cheetah Digital (formerly Wayin), March 23, 2022; with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022; and with Dorian Daley, Executive Vice President and General Counsel, Oracle, April 15, 2022.

213 Human Rights Watch email correspondence with Amy Lee Stewart, Senior Vice President, General Counsel and Chief Privacy Officer, LiveRamp, April 7, 2022; with David Reckert, Managing Privacy Counsel, LiveRamp, April 13, 2022.

214 Human Rights Watch email correspondence with David Reckert, Managing Privacy Counsel, LiveRamp, April 13, 2022.

215 Human Rights Watch email correspondence with Havona Madama, Chief Data Privacy Officer and General Counsel, Bombora, April 5, 2022.

216 Human Rights Watch email correspondence with Elissa Hill, Manager, Global Brand Marketing & Communications, Piano, April 7, 2022.

Influencing Information, Shaping Beliefs

The use of children's personal information to deliver highly targeted content and advertisements that follow them across the internet plays an enormous role in shaping children's experiences and what they see online. This can influence, modify, and manipulate their thoughts and beliefs, nudging them to particular outcomes and possibly affecting their ability to make autonomous choices.[217]

Every child has the right to freedom of thought, and the right to access to information.[218]

Unlike the rights to freedom of expression, association, and assembly, which can be limited, freedom of thought is an absolute right. International human rights law protects children's freedom of thought unconditionally from interference from any lawful or unlawful measure.[219] While the law on this right is underdeveloped, some experts have recently argued that targeted behavioral advertising that manipulates people's thoughts may threaten this right for all people, and particularly for children.[220]

The UN Committee on the Rights of the Child has noted that the digital environment "provides a unique opportunity for children to realize the right to access to information…. States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary."[221]

The UN Committee on the Rights of the Child has noted that many automated processes shaping online experiences "may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions toward more extreme content […] or the use of a child's personal information or location to target potentially harmful commercially driven content."[222]

As such, governments "should ensure that all children are informed about, and can easily find, diverse and good quality information online, including content independent of commercial and political interests." Governments should also "ensure that automated search and information filtering, including recommendation systems, do not prioritize paid content with a commercial or political motivation over children's choices or at the cost of children's right to information."[223]

When these automated processes affect the quality of information that children can easily find online, they risk interfering with children's right to freedom of thought.[224]

Because children are at high risk of manipulative interference at a time when their capacities are evolving, they may be particularly vulnerable when they come into contact with algorithms that

217 UN General Assembly, Interim Report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed, Freedom of thought, A/76/380, October 5, 2021,https://www.ohchr.org/en/issues/freedomreligion/pages/annual.aspx (accessed December 15, 2021), paras. 73-75.

218 Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, arts. 14, 17.

219 CRC, art. 14; Universal Declaration of Human Rights (UDHR), adopted December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), art. 18; see also International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976,, arts. 18(1), 19(1); CRC General Comment No. 1, Article 29(1): The Aims of Education, CRC/GC/2001/1 (2001), para. 8; UN Human Rights Committee, "General Comment Adopted by the Human Rights Committee Under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights," General Comment No. 22 (48) (art. 18), CCPR/C/21/Rev.1/Add.4 (1993), paras. 1, 3; UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 22, 2015, https://www.undocs.org/A/HRC/29/32 (accessed December 15, 2021), para. 19.

220 The UN Special Rapporteur on the right to freedom of religion or belief in a report on the Freedom of thought states that, "Some scholars define manipulation of thought as 'interference with the processes of understanding' to induce the formation of 'biased mental models […], knowledge and ideologies', or a form of 'cognitive mind control.' See: UN General Assembly, Interim Report of the Special Rapporteur on freedom of religion or belief, A/76/380, October 5, 2021, https://www.ohchr.org/en/issues/freedomreligion/pages/annual.aspx (accessed December 15, 2021), paras. 35-39; 73-75.

221 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 50; CRC, art. 14; ICCPR, art. 19(2),(3); UDHR, art. 19; UN General Assembly, "Calling of an International Conference on Freedom of Information," Resolution 59 (1946), A/RES/59.

222 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 40.

223 Ibid, para. 53.

224 Ibid, para. 61.

can be used to target and influence their thoughts, opinions, and beliefs through the curated display of content.[225]

As a result, the UN Committee on the Rights of the Child has urged governments to identify, define and prohibit practices that "manipulate or interfere with" children's freedom of thought. It has also said that governments should ensure that "automated processes of information filtering systems, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment."[226]

The majority of government-endorsed EdTech apps and websites examined by Human Rights Watch sent information about children to Google and Facebook, two companies that not only dominate the advertising and analytics industries, but also serve as primary channels to the internet for much of the world and whose algorithms determine what many people—and children—see online.

SDKs that Human Rights Watch observed most commonly embedded in EdTech apps

SDK	Parent company	EdTech App Count
Google Firebase Analytics	Google	56
Google Crashlytics	Google	40
Facebook Login	Facebook	20
Facebook Share	Facebook	17
Facebook Analytics	Facebook	16
Google AdMob	Google	13
Google Analytics	Google	11
AppsFlyer	AppsFlyer	6
Facebook Places	Facebook	5
Google Tag Manager	Google	5

Third-party companies that Human Rights Watch observed most commonly receiving children's data from EdTech websites through trackers

Parent company	Number of trackers found in EdTech websites
Google	319
Facebook	73
Twitter	59
Adobe	34
Microsoft	34
HubSpot	20
New Relic	18
Hotjar	16
Naver	15
Yandex	15

225 The Council of Europe's Committee of Ministers warned that "fine grained, sub-conscious and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions." See: "Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes," Decl (13/02/2019)1, February 13, 2019, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680092dd4b (accessed July 22, 2021), para. 9. In 2018, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also noted that the "intersection of technology and content curation raises novel questions about the types of coercion or inducement that may be considered an interference with the right to form an opinion," and that "[c]ommercial advertising has also sought to induce favourable opinions of and cultivate desire for particular products and services." He concludes that "[c]ompanies should, at the very least, provide meaningful information about how they develop and implement criteria for curating and personalizing content on their platforms, including policies and processes for detecting social, cultural or political biases in the design and development of relevant artificial intelligence systems." See UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/73/348, August 29, 2018, https://www.undocs.org/A/73/348 (accessed July 22, 2021), paras. 24, 36.

226 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 61-62.

Third-party companies that Human Rights Watch observed most commonly receiving children's data from EdTech websites through cookies

Parent company	Number of cookies found in EdTech websites
Google	99
Microsoft	46
Mail.Ru Group, OOO	25
Pipefy	16
The Trade Desk	16
WiderPlanet	16
LiveRamp	10
Oracle	10
tawk.to	10
Workable	10

In countries and contexts where these companies are viewed as indistinguishable from the internet, the existence of behavioral advertising aimed at children and fueled by data collected in educational contexts risks affecting children's rights to access diverse and good quality information online, including content independent of commercial interests.

Facebook (Meta)

Facebook, which rebranded itself as Meta in October 2021, is the world's dominant social media company.[227] It owns four of the world's biggest social media platforms, and reported over 3.51 billion monthly users across all of its products in the second quarter of 2021.[228] In 2014, Iris Oriss, Facebook's head of localization and internationalization, wrote, "Awareness of the Internet in developing countries is very limited. In fact, for many users, Facebook is the internet, as it's often the only accessible application."[229]

Due to Facebook's ubiquity, its News Feed algorithm, which determines what each of its 2.9 billion users see every day by providing them with a personalized, constantly updated stream of content and advertisements, plays a significant role in influencing people's opinions and beliefs by shaping the information they see online.[230]

Facebook uses the vast amounts of data it has on people to continually train its News Feed algorithm to choose and show content that each person is most likely to engage with. In an internal report from 2018, Facebook found that its recommendation algorithm stoked polarization. "Our algorithms exploit the human brain's attraction to divisiveness," read a slide from the 2018 presentation. "If left unchecked," it warned, Facebook would feed users "more and more divisive content in an effort to gain user attention & increase time on the platform."[231]

227 This report refers to Facebook as both the platform and the parent company, for consistency across the timeline of this investigation.

228 Facebook (Meta) owns four of the world's biggest social media platforms, listed here in descending order of users: Facebook, WhatsApp, Instagram, and Facebook Messenger. See: "Facebook Reports Second Quarter 2021 Results," Facebook press release, July 28, 2021, https://web.archive.org/web/20210807050055/https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter-2021-Results/default.aspx (accessed August 6, 2021); see also Statista, "Most popular social networks worldwide as of April 2021, ranked by number of monthly active users (in millions)," April 2021, https://web.archive.org/web/20210725061434/https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed July 22, 2021).

229 Iris Orriss, "The Internet's Language Barrier," *Innovations: Technology, Governance, Globalization* vol. 9 no. 3-4 (2014): accessed July 20, 2021, doi: 10.1162/inov_a_00223, p. 125. See also: Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar," Facebook, November 8, 2018, https://web.archive.org/web/20210808183551/https://about.fb.com/news/2018/11/myanmar-hria/ (accessed August 8, 2021), p. 12; Saira Asher, "Myanmar coup: How Facebook became the 'digital tea shop,'" BBC, February 4, 2021, https://www.bbc.com/news/world-asia-55929654 (accessed May 6, 2022); Leo Mirani, "Millions of Facebook users have no idea they're using the internet," *Quartz*, February 9, 2015, https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/ (accessed May 6, 2022).

230 In 2010, Eli Pariser coined the term "filter bubble" to describe how personalized recommendation algorithms like those owned by Google and by Facebook reinforce users' beliefs by showing them more of what they prefer, based on their previous activities online. See Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2012).

231 Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," *Wall Street Journal*, May 26, 2020, https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499 (accessed August 9, 2021).

This became reality in Myanmar, "a context where, for most users, Facebook is the Internet."[232] Given its prominence as the online population's primary source of information, Facebook's failure to prevent the spread of hate speech and disinformation that violated its policies on its platform resulted in the company playing what a UN-backed fact-finding mission later called "a determining role" in inciting real world violence in 2018.[233]

In September 2021, a trove of internal documents leaked by the whistleblower Frances Haugen and first published in the Wall Street Journal indicated that over three years, the company's researchers documented Instagram harming the mental and emotional health of a significant number of its child users. Instagram's recommendation algorithm and the negative social comparisons that it stoked made body image issues worse for one in three girls, according to the documents; one slide from a 2019 presentation read, "Teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups."[234]

In response, Facebook's Vice President of Global Affairs, Nick Clegg, said that the Wall Street Journal's reporting "contained deliberate mischaracterizations of what we are trying to do, and conferred egregiously false motives to Facebook's leadership and employees," and suggested that they "need[ed] more evidence to understand social media's impact on people."[235] Nine days later, Facebook paused the development of an Instagram Kids service for children ages 13 and under.[236]

Facebook uses its insights into its users to help advertisers target advertising to people in ways that are optimized to be persuasive to them.[237] This significantly affects what people see on the platform. Over time, Facebook has increased the prevalence of advertising in its News Feed; a 2021 *Wall Street Journal* analysis of Facebook's investor calls found that the company had increased the number of ads served on its platforms by a quarterly average of nearly 30 percent year on year since the third quarter of 2015.[238] Simultaneously, Facebook has also increased the visual prominence and space taken up by ads in the News Feed, continually revising its ad formats to not only make them more prominent and attractive for users, but to integrate them to

232 UN Human Rights Council, "Report of the independent international fact-finding mission on Myanmar," A/HRC/39/64, September 12, 2018, https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf (accessed August 8, 2021), para. 74.

233 Ibid.; Tom Miles, "U.N. investigators cite Facebook role in Myanmar crisis," *Reuters*, March 12, 2018, https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN (accessed August 8, 2021). Facebook commissioned an assessment of its human rights impact in Myanmar, which found that the company had failed to prevent use of the platform to "foment division and incite offline violence." See: Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar," Facebook, November 8, 2018, https://web.archive.org/web/20210808183551/https://about.fb.com/news/2018/11/myanmar-hria/ (accessed August 8, 2021).

234 The majority of internal studies on Instagram's effects on young users were conducted on teenagers in the United States and in the United Kingdom; one spring 2020 study surveyed 100,000 users in Australia, Brazil, France, Germany, Great Britain, India, Japan, Republic of Korea, and the US. See: Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *Wall Street Journal*, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 (accessed November 1, 2021). See also: Nilesh Christopher and Andrew Deck, "Instagram impacts teen mental health in the West. What about everywhere else?" *Rest of World*, November 17, 2021, https://restofworld.org/2021/instagram-teen-mental-health/ (accessed November 18, 2021).

235 Nick Clegg, "What the Wall Street Journal Got Wrong," Meta, September 18, 2021, https://about.fb.com/news/2021/09/what-the-wall-street-journal-got-wrong/ (accessed May 4, 2022).

236 Adam Satariano and Ryan Mac, "Facebook Delays Instagram App for Users 13 and Younger," New York Times, September 27, 2021, https://www.nytimes.com/2021/09/27/technology/facebook-instagram-for-kids.html (accessed May 4, 2022).

237 Facebook advertises this ability to advertisers as, "Personalize every ad for every customer, automatically: Use dynamic ads that automatically show people items they're most interested in." See: Facebook, "Facebook for Business: Retargeting," https://web.archive.org/web/20210809232002/https://www.facebook.com/business/goals/retargeting (accessed August 9, 2021).

238 Laura Forman, "Facebook Ads Could Be Reaching Saturation Point," *Wall Street Journal*, November 23, 2020, https://www.wsj.com/articles/facebook-ads-could-be-reaching-saturation-point-11606132807 (accessed July 20, 2021).

239 In an earnings call with investors in January 2013, Facebook CEO Mark Zuckerberg announced a substantial redesign of the News Feed to make ads more visually prominent and attractive, explaining the change as, "Advertisers want really rich things like big pictures or videos, and we haven't provided those things historically." See: Somini Sengupta, "Face-Lift at Facebook, to Keep Its Users Engaged," *New York Times*, March 6, 2013, https://www.nytimes.com/2013/03/07/technology/facebooks-redesign-hopes-to-keep-users-engaged.html (accessed August 9, 2021); Facebook, "A New Look for News Feed," March 7, 2013, https://web.archive.org/web/20210809223518/https://about.fb.com/news/2013/03/a-new-look-for-news-feed/ (accessed August 9, 2021). In 2015, Andrew Bosworth, Vice President of Ads and Business Platform, described Facebook's shift to native ads—defined as ads that blend into content by matching the format or tone of the platform they appear on, making it more difficult for users to identify them as ads—as "It's about the ads not being in the right-hand column, but being a part of News Feed and having voice and actors and Likes and comments in the same way that you see this with other content in News Feed." Cade Metz, "How Zuck's Old TA Helped Facebook Master Mobile Ads," *WIRED*, September 21, 2015, https://www.wired.com/2015/09/zucks-old-ta-helped-facebook-master-mobile-ads/ (accessed July 20, 2021).

further blur the lines between advertisements and organic content.[239]

As described in the previous section, children are at heightened risk of being influenced by behavioral advertising on social media sites like Facebook, where the lines between organic and commercial content are blurred and advertisements take up significant real estate in the News Feed.

In April 2021, Reset Australia, an advocacy group, reported that Facebook offered advertisers the ability to target their ads to approximately 740,000 children in Australia, and to target children as young as 13 determined by Facebook to be interested in smoking, extreme weight loss, and gambling, for as little as AU$3.03.[240] A Facebook spokesperson said that the company reviews all ads before and after they run, and that advertisers must comply with Facebook's policies and local laws.[241]

The news outlet the *Australian* reported in 2017 that a leaked Facebook document showed the company telling advertisers that it could judge when teenagers were feeling "insecure" and "worthless," and offering advertisers the ability to target ads at the moment when young people "need a confidence boost." The document, which stated that the company held data on 1.9 million *Australian* high schoolers, included an analysis on how young people express their emotions at different points during the week.[242] In response, Facebook first released a statement to the Australian in which it apologized and said it would undertake disciplinary measures;[243] it released a second statement that said the article's premise was misleading, that it does not offer tools to target people based on their emotional state, and that the document was commissioned research that was never used to target ads and was based on anonymous and aggregated data.[244]

Not including Facebook's own app and website, Human Rights Watch detected 62 EdTech products with embedded Facebook tracking technologies.[245] Of these, 22 apps had installed Facebook's SDKs, giving the company the ability to access children's personal data, and 37 websites were found transmitting children's data to Facebook through ad trackers, third-party cookies, and the Facebook Pixel.

Facebook Pixel

Human Rights Watch found 31 EdTech websites sending their users' data to Facebook through a specific tracking technology known as the Facebook Pixel. This technology collects information about what students and teachers do on these sites and sends this data back to Facebook. This can be used by the EdTech website to later target them with ads on Facebook and Instagram.

Facebook can also retain and use this data for its own advertising purposes, although it is not always clear what these purposes are.[246] The Facebook Pixel allows Facebook to track people across the internet, and build user profiles on people – even matching them and their data to their respective Facebook or Instagram profiles, if they have one, and even if they are not logged into Facebook at the time when they were accessing a website with an embedded Facebook Pixel.[247] As noted previously in this report, the Facebook Pixel could

240 Reset Australia, "Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data," April 2021, https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf (accessed July 13, 2021), p. 2, 13.

241 Conor Duffy, "Facebook approves alcohol, vaping, gambling and dating ads targeting teens, lobby group finds," ABC News, April 27, 2021, https://www.abc.net.au/news/2021-04-28/facebook-instagram-teenager-tageted-advertising-alcohol-vaping/100097590 (accessed May 5, 2022).

242 Darren Davidson, "Facebook targets 'insecure' young people to sell ads," *Australian*, May 1 2017, http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6 (accessed July 13, 2021), Sam Levin, "Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless,'" Guardian, May 1, 2017, https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens (accessed July 13, 2021).

243 Darren Davidson, "Facebook targets 'insecure' young people to sell ads," *Australian*, http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

244 Facebook, "Comments on Research and Ad Targeting," April 30, 2017, https://about.fb.com/news/h/comments-on-research-and-ad-targeting/ (accessed July 13, 2021).

245 Facebook tracks people on its website and app by using its own internal tools. For an explanation, see: Aaron Sankin and Surya Mattu, "I Scanned My Favorite Social Media Site on Blacklight And It Came Up Pretty Clean. What's Going On?" *The Markup*, October 1, 2020, https://themarkup.org/ask-the-markup/2020/10/01/i-scanned-my-favorite-social-media-site-on-blacklight-and-it-came-up-pretty-clean-whats-going-on (accessed July 13, 2021).

246 Surya Mattu and Colin Lecher, "Applied for Student Aid Online? Facebook Saw You," *The Markup*, April 28, 2022, https://themarkup.org/pixel-hunt/2022/04/28/applied-for-student-aid-online-facebook-saw-you (accessed May 5, 2022).

247 Ibid. Facebook describes the pixel as "The Facebook pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts." See: Facebook, "Facebook Pixel: Implementation," https://web.archive.org/web/20210713213425/https://developers.facebook.com/docs/facebook-pixel/implementation (accessed July 13, 2021); see also: Surya Mattu et al., "How We Built a Meta Pixel Inspector," *The Markup*, April 28, 2022, https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (accessed May 5, 2022).

also enable the company to collect personal data and create shadow profiles on people who have never used their services or signed up for an account.

Of the 31 EdTech websites found by Human Rights Watch to be sending data to Facebook through Facebook Pixel, 27 are websites specifically designed for use by children, and all were government-recommended for online learning. Facebook could use such data to profile children and target behavioral advertisements at them.

Product	Country	Child specific?
Educ.ar	Argentina	Yes
Education Perfect: Science	Australia: Victoria	Yes
DragonLearn	Brazil: São Paulo	Yes
Mangahigh	Brazil: São Paulo	Yes
Descomplica	Brazil: São Paulo	Yes
Escola Mais	Brazil: São Paulo	Yes
Explicaê	Brazil: São Paulo	Yes
Stoodi	Brazil: São Paulo	Yes
StoryWeaver	Canada: Quebec	Yes
CBC Kids	Canada: Quebec	Yes
Active for Life	Canada: Quebec	No
Dropbox	Colombia	No
Khan Academy	India: Uttar Pradesh, Pakistan, Nigeria, South Africa	Yes
WeSchool	Italy	Yes
Study Sapuri	Japan	Yes
Z-kai	Japan	Yes
eboard	Japan	Yes
Asahi Shimbun	Japan	No
Daryn Online	Kazakhstan	Yes
iTest	Kazakhstan	Yes
Learn Smart Pakistan	Pakistan	Yes
Sabaq Foundation	Pakistan	Yes

EBS	Republic of Korea	Yes
ExamenulTau	Romania	Yes
Kinderpedia	Romania	Yes
Miro	Romania	No
ȘcoalaIntuitext	Romania	Yes
Moscow Electronic School	Russia	Yes
Siyavula	South Africa	Yes
PaGamO	Taiwan	Yes
ST Math	US: Texas	Yes

In July 2021, Facebook announced that advertisers would no longer be able to use Facebook's full suite of detailed targeting capacities when targeting children; instead, advertisers would be limited to targeting children based on their age, gender, and location.[248] The announcement came two months after 44 state attorneys general in the US wrote to Facebook CEO Mark Zuckerberg asking him to abandon his plans to create an Instagram service for children under the age of 13, citing social media's detrimental effect on the health and well-being of children and the company's track record of having "historically failed to protect the welfare of children on its platforms."[249]

Facebook did not commit to limiting its own collection, profiling, and targeting of children for its own purposes. Its new policy does not protect children from advertisements targeted to people "living in this location," "recently in this location," or "traveling in this location," as well as to infer further sensitive information about children as described in Chapter 2.[250]

When reached for comment, Facebook did not acknowledge that they receive data from the EdTech products listed by Human Rights Watch, and said that it was their customers' responsibility to comply with their policies and applicable laws that prohibit the collection of children's data.[251]

For children aged 13-17 with a user account with one of Facebook's services, the company said that it "does not use data from our advertisers' and partners' websites and apps to personalize [ads] to people under 18," and also confirmed that advertisers can only target ads to children aged 13-17 based on age, gender, and location. Facebook also said that children under 13 were not authorized to sign up for an account to use its products, and therefore if the company "were to inadvertently receive data relating to a child under 13, there would not be an authorized Meta user account for that child to which the data could be connected."[252]

An internal document written by Facebook's privacy engineers on the Ad and Business Product team and published by *Vice* in April 2022 suggests that the company struggles to understand and track how people's data are shared and used inside of its own systems. "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose,'" the document said.[253] In response to the internal document, Facebook said that the document did not demonstrate non-compliance with privacy regulations, because it did not describe the company's processes and controls to comply with privacy regulations.[254]

248 Facebook, "Giving Young People a Safer, More Private Experience," July 27, 2021, https://web.archive.org/web/20210729194429/https://www.facebook.com/business/news/facebook-is-changing-how-advertisers-can-reach-young-people (accessed August 10, 2021); Facebook, "About Advertising to Young People," Facebook Business Help Center, https://web.archive.org/web/20210728001952/https://www.facebook.com/business/help/229435355723442 (accessed July 28, 2021).

249 National Association of Attorneys General, "Letter Re: Facebook's Plans to Develop Instagram for Children Under the Age of 13," May 10, 2021, https://ag.ny.gov/sites/default/files/naag_letter_to_facebook_-_final.pdf (accessed August 2, 2021).

250 Facebook, "Use Location Targeting," Facebook Business Help Center, https://www.facebook.com/business/help/365561350785642?id=176276233019487 (accessed August 2, 2021).

251 Human Rights Watch email correspondence with Miranda Sissons, Director, Human Rights Policy, Meta, April 15, 2022.

252 Ibid.

253 Lorenzo Franceschi-Bicchierai, "Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document," *Vice*, April 26, 2022, https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes (accessed May 5, 2022).

254 Ibid.

Google

Mr. Google has sucked in a beastly amount of information during these days.

—Pere Nieto, primary school teacher, Barcelona, Spain[255]

Google holds unparalleled dominance over the world's digital advertising market. According to public data, the company has been the global market leader in online advertising for over a decade, commanding a 27.5 percent share of digital ad spending in 2021.[256] In turn, advertising contributes to the majority of Google's business; in 2020, it reported that 80 percent of its total annual revenue, or US$147 billion, was earned by its ads business.[257]

Google's considerable control over online advertising is reinforced by the overwhelming market dominance of its other services, which have become essential to how most people participate in life online. Google is by far the most widely used search engine in the world; over 92 percent of all internet queries worldwide are done through Google, and to "Google" something is synonymous with online search itself.[258] As such, the company's algorithms determine what most people see when they search for information on the internet, as well as the digital ads displayed alongside their search results.

Nine of the company's products—Android, Chrome, Gmail, Google Drive, Google Maps, Google Play Store, Google Photos, Google Search, and YouTube—have more than a billion users each.[259] Each of these products provides vast amounts of user data back to Google, which analyzes this data to create new insights and information about people that can then be sold to advertisers.[260]

The company collects data not just from people directly using their services, but from anyone who encounters their tracking technologies embedded across the internet. Google offers infrastructure and developer tools that are popularly used by other companies to build their own websites and apps; many of these tools offer multiple capabilities, including advertising.[261] When using Google's services, developers provide Google with their

255 Human Rights Watch interview with Pere Nieto, primary school teacher, Barcelona, Spain, June 12, 2020.

256 Ethan Cramer-Flood, "Duopoly still rules the global digital ad market, but Alibaba and Amazon are on the prowl," *eMarketer*, May 10, 2021, https://www.emarketer.com/content/duopoly-still-rules-global-digital-ad-market-alibaba-amazon-on-prowl (accessed August 9, 2021).

257 Google filing to United States Securities and Exchange Commission (SEC), "Form 10-K, Annual Report for the fiscal year ended December 31, 2020," https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d (accessed August 9, 2021), p. 10.

258 StatCounter, "Search Engine Market Share Worldwide: Aug 2020-Aug 2021," https://web.archive.org/web/20210908155103/https://gs.statcounter.com/search-engine-market-share (accessed September 8, 2021).

259 Harry McCracken, "How Google Photos joined the billion-user club," Fast Company, July 24, 2019, https://www.fastcompany.com/90380618/how-google-photos-joined-the-billion-user-club (accessed September 8, 2021).

260 Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights," November 21, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/ (accessed May 5, 2021).

261 Research conducted by AppCensus for the Australian Competition and Consumer Commission found that Google's SDKs—those with advertising and analytics capacities—were embedded in 91 percent of 1,000 of the most popular mobile apps in Australia, and in 72 percent of children's apps. See: AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC," September 24, 2020, https://www.accc.gov.au/system/files/1%2C000%20Mobile%20Apps%20in%20Australia%20%E2%80%93%20A%20Report%20for%20the%20ACCC%2C%20AppCensus_0.pdf (accessed July 9, 2021) pp. 22-26.

262 Google, "How Google uses information from sites or apps that use our services," https://web.archive.org/web/20210915110048/https://policies.google.com/technologies/partner-sites (accessed September 15, 2021).

263 For example, Google Firebase Analytics offers developer tools for building and maintaining apps. It was the most prevalent SDK found in EdTech apps analyzed by Human Rights Watch, and is similarly ubiquitous in Android apps worldwide. Firebase also offers developers the capability to use their users' personal data to "gain insight into who your users are, and what actions they're taking inside your app," and to "apply the power of machine learning to predict future user behavior." Once collected and analyzed by Firebase, users' personal data can be sent to and integrated with Google's other advertising services, including Google Ads, AdMob, and Google Marketing Platform. See: Google Firebase, "Products / Engage," https://web.archive.org/web/20210811171053/https://firebase.google.com/products-engage (accessed August 11, 2021); Google Firebase, "Integrations," https://web.archive.org/web/20210811171551/https://firebase.google.com/integrations (accessed August 11, 2021); Google Firebase, "AdMob and Firebase," April 19, 2022, http://web.archive.org/web/20220429083336/https://firebase.google.com/docs/admob (accessed May 5, 2022).

users' data.[262] Google offers developers the ability to collect users' data through its non-advertising specific tools and integrate it later with its advertising services.[263]

Google's advertising ecosystem is opaque, and even experts struggle to understand how its algorithms use the data they collect or receive about people to decide what to show them online.[264] It is difficult to know how personal data is used within Google's ecosystem once it is collected, and difficult to distinguish between "where Google as a service provider ends, and where Google as an advertising service begins."[265]

Of the 164 EdTech products examined by Human Rights Watch, 132 products (80 percent) were found with embedded tracking technologies built by Google.[266] Of these, 63 Android apps (86 percent of the total 73 apps examined) were found with at least one embedded Google SDK, giving the company the ability to access children's personal data based on the Android permissions also granted to the app. Human Rights Watch observed 101 websites (81 percent of the total 125 websites examined) transmitting children's data to Google through ad trackers, third-party cookies, and Google Analytics' 'remarketing audiences' feature.

Human Rights Watch also further identified instances in which EdTech products sent or granted access to children's data directly to Google's advertising divisions, which Google may use for its own purposes.[267]

For example, Google Analytics is popularly used for both its analytics and advertising capabilities. Human Rights Watch examined websites identified to be using a tool offered by Google Analytics, called its 'remarketing audiences' feature, that allows developers to make custom audience lists based on user behavior and then target ads to those users across the internet using Google Ads and Display & Video 360.[268]

EdTech products sent or granted access to children's data to Google, using Google's advertising-specific tracking technologies

EdTech Type	Tracker	Receiving Domain	Number of EdTech products
Apps	SDK	Google AdMob	14
	SDK	Google Tag Manager	5
Websites	Ad Tracker	googletagmanager.com	65
	Ad Tracker	doubleclick.net	64
	Ad Tracker	googleadservices.com	31
	Ad Tracker	googletagservices.com	7
	Ad Tracker	googleoptimize.com	2
	Cookie	doubleclick.net	43
	Cookie	10499192.fls.doubleclick.net	1
	Google Analytics' 'remarketing audiences' feature	stats.g.doubleclick	53

Of the 73 EdTech apps reviewed in this report, Human Rights Watch found that 17 apps (23 percent) had installed one of Google's ad-specific SDKs; likewise, out of the total 125

264 Norwegian Consumer Council ("Forbrukerrådet"), "Out of Control," January 14, 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/ (accessed June 10, 2021), p. 121. Despite the extreme difficulties of knowing when and what influences Google's ads ecosystem and its proprietary algorithmic design, researchers and journalists have been working to catalog and analyze its outputs. See: Leon Yin and Aaron Sankin, "Google Ad Portal Equated 'Black Girls' with Porn," *The Markup*, July 23, 2020, https://themarkup.org/google-the-giant/2020/07/23/google-advertising-keywords-black-girls (accessed September 15, 2021); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018); Latanya Sweeney, "Discrimination in Online Ad Delivery," January 28, 2013, https://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf (accessed September 15, 2021).

265 Norwegian Consumer Council ("Forbrukerrådet"), "Out of Control," https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, p. 120.

266 As noted in the methodology, several EdTech products offered both app and website versions of their product, in which case Human Rights Watch analyzed both.

267 "Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners' sites and apps." See: Google, "How Google uses information from sites or apps that use our services," https://web.archive.org/web/20210915110048/https://policies.google.com/technologies/partner-sites (accessed September 15, 2021).

268 Surya Mattu and Aaron Sankin, "How We Built a Real-time Privacy Inspector," *The Markup*, September 22, 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector (accessed July 7, 2021); Google Analytics, "Tracking Code Overview," https://web.archive.org/web/20200615214845/https:/developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview (accessed July 7, 2021).

269 These are defined as any network requests that were made to the following Google-owned domains: Google Analytics, Google Tag Manager, DoubleClick, googleadservices.com, googlesyndication.com, and googletagservices.com.

EdTech websites reviewed, 83 websites (66 percent) were found transmitting children's personal data to Google's advertising businesses.[269]

For example, Human Rights Watch found 14 apps granting access to their users' data to Google AdMob by installing the AdMob SDK, "one of the largest global ad networks" that "helps you monetize your mobile app through in-app advertising."[270] Ten out of the 14 are apps designed specifically for children's use in education, and their data sharing practices directly impacted children.[271]

Google's advertising policies prohibit targeting children under 13 with behavioral advertising or collection of their personal information for that purpose.[272] Google places responsibility on the developer to follow these policies: "You are responsible for ensuring your ads comply with policy where required," but the company does not appear to have a due diligence policy to actively check whether the personal data they receive might be that of children.[273]

In August 2021, Google announced that it would no longer allow advertisers to target personalized advertising to children based on their age, gender, or interests.[274] However, the company did not preclude advertisers from continuing to use location data to infer sensitive information and target ads to children.[275] The company also did not comment on the massive amounts of children's personal data that it has received to date, nor did it commit to limiting its own collection of children's data or its profiling and targeting of children.

Through dynamic analysis, Human Rights Watch detected one EdTech app, e-Pathshala, transmitting details about what children search for within the app to Google. The Indian Education Ministry, who built the app, does not notify its child users that the app is sending what information children seek within their virtual classroom to Google. Indeed, the app has no privacy policy at all.

Neither Google nor e-Pathshala responded to our request for comment.

270 Google AdMob, "Home," https://admob.google.com/home/ (accessed August 11, 2021); Google Developers, "AdMob," https://developers.google.com/admob (accessed August 11, 2021).

271 These apps were: Top Parent, Descomplica, Edmodo, Study Sapuri, (LINE), Özelim Eğitimdeyim, Extramarks, (Naver Band), Newton, Minecraft, (Miro), Kundelik. Apps in parentheses are directed at general audiences; the rest are apps apparently designed for use by children.

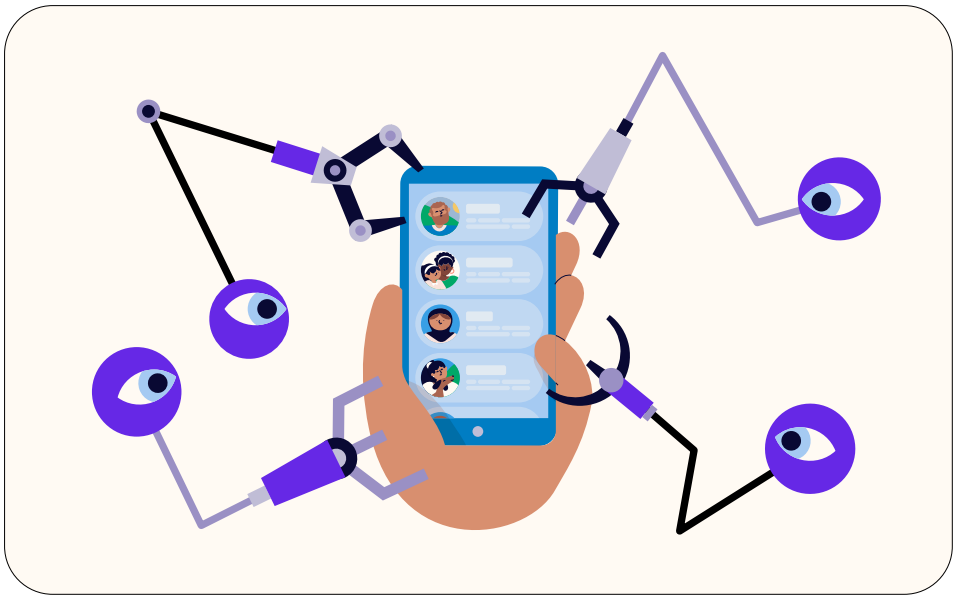
272 Google, "Personalized advertising," https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465 (accessed August 11, 2021); Google, "Ads & made for kids content," https://web.archive.org/web/20210811183721/https://support.google.com/adspolicy/answer/9683742?hl=en&ref_topic=1626336 (accessed August 11, 2021).

273 Google, "Personalized advertising," https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465.

274 Mindy Brooks, "Giving kids and teens a safer experience online," post to Google: The Keyword (blog), August 10, 2021, https://web.archive.org/web/20210810130430/https://blog.google/technology/families/giving-kids-and-teens-safer-experience-online/ (accessed August 10, 2021).

275 In 2018, an AP investigation concluded that Google collects location data from Android users, even if users had set their privacy settings to prevent Google from doing so. The Attorney General of the US state of Arizona subsequently filed a consumer fraud lawsuit against Google in May 2020; newly unredacted documents in May 2021 revealed testimony from Jack Menzel, Google's former Vice President of Product for Maps and current Vice President of Product for ads, that Google infers a user's home and work locations without consent, even when a user has turned off all of their device's location-related settings, and that the only way for Google not to infer a user's home and work locations is to insert " arbitrary locations." Karin Hennessy, Google's product manager for ads privacy and safety, similarly noted during deposition that even if a user opts out of ads personalization, Google still uses the user's real-time location to serve ads to them. See: Ryan Nakashima, "AP Exclusive: Google tracks your movements, like it or not," *Associated Press*, August 13, 2018, https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1afoecb (accessed August 11, 2021); *State of Arizona Attorney General, Mark Brnovich v. Google LLC*, The Superior Court of the State of Arizona In and For The County of Maricopa, Complaint, May 2021, https://www.azag.gov/sites/default/files/2021-05/Complaint%20%28redacted%29.pdf (accessed August 11, 2021), paras. 93, 99; Google, "Personalized Advertising," https://web.archive.org/web/20210811183214/https://support.google.com/adspolicy/answer/143465 (accessed August 11, 2021).

IV. Failure to Protect



This is scary. Especially us kids, we blindly trust our country, the whole education system, because we don't question these things yet. We don't have enough experience.... As kids, we feel powerless. What can I even do as a kid to stop these companies? That idea itself hurts a lot.

—Priyanka S., 16, Uttar Pradesh, India[276]

Companies' and Governments' Child Rights Responsibilities

Companies have a responsibility to respect all children's rights, wherever they operate in the world and throughout their operations.[277] This is a widely recognized standard of expected corporate conduct, as set out in international human rights standards including the United Nations Guiding Principles on Business and Human Rights, and by the UN Committee on the Rights of the Child.[278]

Companies' responsibilities encompass preventing their services from being used in ways that cause or contribute to violations of children's rights, even if they were not directly involved in perpetrating abuses.[279] These responsibilities hold even when a national government lacks the necessary laws and regulations to sanction such abuses, or is unable or unwilling to protect children's rights.[280]

Governments are responsible for ensuring that businesses meet these responsibilities.[281] They have a duty to protect children and their rights, and so should prevent, monitor, investigate, and punish child rights abuses by businesses. Governments are themselves also held responsible for violating children's rights if they have failed to take necessary, appropriate, and reasonable measures to prevent and remedy such violations, or otherwise tolerated or contributed to these violations.[282]

276 Human Rights Watch interview with Priyanka S., 16, Uttar Pradesh, India, August 2, 2021.

277 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 35.

278 United Nations Human Rights Council, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," adopted on July 6, 2011, A/HRC/RES/17/4, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed August 2, 2021); OECD, OECD Guidelines for Multinational Enterprises: 2011 Edition, May 25, 2011, https://www.oecd.org/daf/inv/mne/48004323.pdf (accessed August 2, 2021); CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 35.

279 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 36; UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, Principle 13(b).

280 UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, Principles 11, 13.

281 CRC, General Comment No. 16, State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16 (2013), paras. 28, 42; CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 35, 36.

282 CRC, General Comment No. 25, para. 37; CRC, General Comment No. 16, para. 28.

When children's rights are violated in an environment of opaque digital systems, businesses' global operations, and complex flows of data and technology between actors and across jurisdictions, children face immense challenges in finding justice. It is difficult for children, much less adults, to obtain evidence, identify perpetrators, or to even know what their rights are and when they have been abused—particularly if they have to act individually and expose themselves to scrutiny to get action from digital service providers.

Governments are obligated to provide effective remedies for violations of children's rights, and companies have a responsibility to put in place processes to remedy rights abuses which they caused or to which they contributed.[283] Remedies should be widely known and readily available to all children; they should involve prompt, thorough, and impartial investigation of alleged violations, and should be capable of ending ongoing violations.[284]

Child Data Protection Laws

The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care, including legal protections, at all stages of their lives.[285]

Even as more children spend increasing amounts of their childhood online, most countries in the world do not have modern child data protection laws that would provide protections to children in complex online environments. For example, of the 49 countries examined by Human Rights Watch in this report, 14 countries had no data protection laws at all. Twenty-four countries possessed data protection laws that contained references to children, but these were restricted to the question of who may provide consent to the processing of children's data. Some of these were written at a time when digital technologies and data practices described in this report did not exist. For example, the United States' Children's Online Privacy Protection Act, signed into law in 1998 and subsequently amended, does not provide protections to children aged 13 to 18, nor restrict companies from collecting and using children's data for purposes not in the best interest of the child, including commercial interests and behavioral advertising.[286] This domestic law has impacted children's digital experiences worldwide due to the fact that many of the largest and most influential technology companies that provide global services—including the majority of AdTech companies covered in this report—are headquartered in the US.

As a result, technology companies have faced little regulatory pressure or incentive to prioritize the safety and privacy of children in the design of their services. Most online service providers do not offer specific, age-appropriate data protections to children, and instead treat their child users as if they were adults.

The majority of EdTech products examined by Human Rights Watch did not offer data protections specific to children, nor did they provide a high level of privacy by design and default. As noted in this report, of the 164 EdTech products reviewed, 146 (89 percent) engaged in data practices that put children's rights at risk, contributed to undermining them, or actively infringed on these rights.

Of the 74 AdTech companies that responded to Human Rights Watch's request for comment, an overwhelming majority did not state that they had operational procedures in place to prevent the ingestion or processing of children's data, or to verify that the data they did receive comply with their own policies and applicable child data protection laws. Absent effective protections, AdTech companies appear to routinely ingest and use children's data in the same way they do adults' data.

283 ICCPR, art. 2(3); UN Human Rights Council, Guiding Principles on Business and Human Rights, adopted on July 6, 2011, A/HRC/RES/17/4, principles 15, 22.

284 ICCPR, art. 2(3); UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, UN Doc. A/HRC/39/29, August 3, 2018, paras. 50-57; UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/73/348, August 29, 2018, https://www.undocs.org/A/73/348 (accessed July 22, 2021), para. 39; CRC, General Comment No. 16, State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16 (2013), para. 4 (c); CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), paras. 43-49.

285 See: Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990.

286 Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506, https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm (accessed May 9, 2022).

The UN Committee on the Rights of the Child states that governments "should review, adopt and update national legislation" to ensure that the digital environment protects children's rights, and that such legislation "should remain relevant, in the context of technological advances and emerging practices."[287] Laws should be updated to specifically support enforcement and compliance in digital environments.[288]

Education

Every child has the right to education. International human rights law makes clear that governments are responsible for ensuring free and compulsory primary education,[289] and governments must fulfill an "unequivocal" requirement to ensure the availability of primary education without charge to children, their parents or guardians, and eliminate all direct and indirect costs to children's education.[290] Governments must make secondary education progressively available and accessible to all children.[291] Human Rights Watch calls on states to take immediate measures to ensure that secondary education is available and accessible to all, free of charge. Human Rights Watch also calls on states to make education compulsory through the end of lower secondary school, in line with the Sustainable Development Goals and the political commitments made by all United Nations member states to provide 12 years of free primary and secondary education, with 9 compulsory years of education.[292]

Education offered to children needs to "promote the realization of the child's other rights,"[293] placing the best interests of students as a "primary consideration."[294] As digital technologies can be used to support children's access to education, the Committee on the Rights of the Child has stated that governments "should ensure that the use of those technologies is ethical and appropriate for educational purposes and does not expose children to … misuse of their personal data, commercial exploitation or other infringements of their rights."[295]

The Abidjan Principles on the human rights obligations of states to provide public education and to regulate private involvement in education, which are guiding principles adopted in 2019 by a group of independent experts from around the world, state that governments should regulate companies providing ancillary services that enable learning to ensure that their actions facilitate, not obstruct, the right to education.[296] They further call on governments to "ban commercial advertising and marketing in public and private instructional educational institutions, and ensure that curricula and pedagogical methodologies and practices are not influenced by commercial interests."[297] Where children rely on services from the private market to access their right to education, states should also ensure that private actors do not infringe on children's other rights, including their rights to privacy; to play; to seek, receive, and impart information; to freedom of expression; and to freedom of thought.[298]

As described in this chapter, some governments made it compulsory for students and teachers to use government-built or endorsed EdTech products during the pandemic. This not only subjected them to the data practices and privacy protections—or lack thereof—of those products, but also made it impossible for children to protect themselves by opting for alternative means to access their right to education.

287 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 23.

288 Ibid., paras. 28-29; 35-39.

289 CRC, art. 28(1)(a); ICESCR, art. 13 (2)(a).

290 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 11: Plans of Action for Primary Education (article 14 of the International Covenant on Economic, Social and Cultural Rights)," UN Doc. E/C.12/1999/4 (1999), https://undocs.org/en/E/C.12/1999/4 (accessed July 23, 2021), para. 7.

291 CRC, art. 28(1)(b); ICESCR, art. 13 (2)(b).

292 United Nations, The 2030 Agenda for Sustainable Development, "UN Sustainable Development Goal 4, Target 4.1.: Free Primary and Secondary Education," https://sdg4education2030.org/the-goal (accessed May 4, 2022).

293 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 11: Plans of Action for Primary Education (art. 14 of the International Covenant on Economic, Social and Cultural Rights)," para. 6.

294 UN Committee on Economic, Social and Cultural Rights, "General Comment No. 13 (Twenty-first session, 1999) The right to education (article 13 of the Covenant)," UN Doc. E/C.12.1999/10 (1999) https://undocs.org/E/C.12/1999/10 (accessed October 25, 2021), para. 7.

295 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 103.

296 "The Abidjan Principles–Guiding Principles on the human rights obligations of States to provide public education and to regulate private involvement in education," 2019, https://www.right-to-education.org/resource/abidjan-principles (accessed February 22, 2020), principle 4, para. 58.

297 Ibid., para. 59.

298 CRC, General Comment No. 25, Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2021), para. 103; OHCHR, "Guiding Principles on Business and Human Rights," 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed April 2, 2021), Principles 1, 13; UN Human Rights Council, Report of the Special Rapporteur on the right to education, "Right to education: impact of the coronavirus disease crisis on the right to education–concerns, challenges and opportunities," UN Doc. A/HRC/44/39 (2020), https://undocs.org/A/HRC/44/39 (accessed November 9, 2021), para. 84 (j).

Students, Parents, and Teachers Operating in Blind Faith

Children, parents, and teachers operated on blind faith that their governments would protect children's rights when providing education online during Covid-19 school closures.

Many children and parents told Human Rights Watch that they did not recall ever being asked for their consent, much less informed how their rights might be protected or affected, when told to adopt specific EdTech products for school.[299] Hayley John, a mother of two in Murwillumbah, Australia, said: "I just trusted the school had looked into it. What would we do about it anyway?... We were worried about the tension and uncertainty around this pandemic, so we were trying to make things work."[300]

But teachers told Human Rights Watch that they were also not informed how the EdTech products they were told to use would protect their students' privacy or told to explain and seek consent from children or their parents.[301] One secondary school teacher in London, United Kingdom, was told by his school to begin teaching in Google Classroom. But regarding the protection of his students' privacy, he said: "I'm not sure what the school has done.[...] I'm not aware that any student has signed any kind of waiver or consent form. I certainly haven't."[302]

Asked whether she had been instructed to seek consent from students and parents, Marie-Therese Exler, a 6th grade teacher in Schleswig-Holstein, Germany, said: "No. I assumed it would be fine and someone else decided over this."[303] A secondary school teacher in Bilbao, Spain, said simply, "If the school's IT team says to use it, it is supposed to be fine."[304]

Some teachers told Human Rights Watch that their government created accounts for them and their students on EdTech platforms without asking for consent or informing them of the products' privacy practices. Fifth-grade teacher Daniela Andrea Ribeiro Espinoza, in Santiago, Chile, said: "The platforms were activated from the Huechuraba education department. They activated everything and sent us an institutional email, no more. We have never been asked to sign or accept anything."[305] When asked whether he was asked to explain or seek consent from his students and their parents, one teacher in Hesse, Germany said: "No. We just got the access code [for the software] and that was it."[306]

"We don't really understand what's going on with data protection," said a primary school teacher in Barcelona, Spain. "The teachers at my school have accepted it, but it is the feeling that the students and teachers know everyone's home, as they have entered them virtually ... I don't know how it would have worked if someone hadn't wanted to [use the EdTech platform]. Being an extraordinary situation, people have accepted it.... There have been zero clear guidelines from the government or the Department of Education."[307]

Some teachers expressed concern for their students' data privacy.[308] Abby Rufer, an algebra teacher in Texas, US, said that her school district initially did not implement protections for students' privacy. "Teachers were using [an online platform] which has no privacy protection. I was worried because, especially for our kids, this is not safe for them. Sixty to seventy percent of our kids had one primary family member that had been deported or was currently in ICE [US Immigration and Customs Enforcement] holding.
So, this is unacceptable, and it is a dangerous situation to put these kids in."[309]

299 Human Rights Watch interviews with Jordi C., 16, Lleida, Catalonia, Spain, June 11, 2020; Gaetana Pacella, mother, Balvano, Italy, June 19, 2020; mother, Sydney, Australia, June 12, 2020; Bilqiis M., mother of two, Hvidovre, Denmark, June 10, 2020; mother, Sidon, Lebanon, June 22, 2020; primary school teacher in Seattle, Washington, United States, June 22, 2020; Pema W., 5th grade mathematics teacher, Dharamsala, India, June 14, 2020.

300 Human Rights Watch interview with Hayley John, Murwillumbah, New South Wales, Australia, June 12, 2020.

301 Human Rights Watch interviews with teacher's assistant, Berkshire, Massachusetts, United States, June 10, 2020; Molly Dobkin, primary school teacher, New York, United States, June 7, 2020; Tanja Ilic, teacher, Požarevac, Serbia, July 1, 2020.

302 Human Rights Watch interview with secondary school teacher, London, United Kingdom, June 12, 2020.

303 Human Rights Watch interview with Marie-Therese Exler, teacher, Kiel, Schleswig-Holstein, Germany, June 3, 2020.

304 Human Rights Watch interview with teacher, Bilbao, Spain, June 12, 2020.

305 Human Rights Watch interview with Daniela Andrea Ribeiro Espinoza, teacher, Santiago, Chile, July 9, 2020.

306 Human Rights Watch interview with #42, teacher, Kassel, Hesse, Germany, June 10, 2020.

307 Human Rights Watch interview with Pere Nieto, teacher, Barcelona, Spain, June 12, 2020.

308 Human Rights Watch interview with teacher, central Iowa, United States, June 18, 2020.

309 Human Rights Watch interview with Abby Rufer, teacher, Dallas, Texas, United States, June 8, 2020.

Companies Failed to Protect

Human Rights Watch found that the data practices of an overwhelming majority of EdTech companies and their products risked or infringed on children's rights. As noted above, companies are responsible for preventing and mitigating abuses of children's rights, including those they indirectly contribute to through their business relationships. Out of 94 EdTech companies, 87 (93 percent) directly sent or had the capacity to grant access to children's personal data to 199 companies, overwhelmingly AdTech, as described in Chapters 2 and 3. In many cases, this enabled the commercial exploitation of children's personal data by third parties, including AdTech companies and advertisers, and put children's rights at risk or directly infringed upon them.[310]

The majority of these companies—79—built and offered educational products designed specifically for children's use. In each of these 80 products apparently designed for use by children, the EdTech company implemented tracking technologies to collect and to allow AdTech companies to collect personal data from children.

Most EdTech companies did not inform children and their parents of how children were secretly surveilled by the online learning platforms they used daily for school. As described in Chapter 2, companies failed to disclose data practices that risked or infringed on children's privacy; 18 companies did not provide a privacy policy at all. As these tracking technologies were invisible to the user, children had no reasonably practical way of knowing the existence and extent of these data practices, much less the impacts on their rights. By withholding critical information, these companies also impeded children's access to justice and remedy.

Case Study: Daryn Online, Kazakhstan

Flush with new users and a captive audience during Covid-19 school closures, EdTech companies faced financial incentives to commercialize children's data and their attention. This was exemplified by Daryn Online, an educational website built by a Kazakh startup, Bugin Soft, which offers classes for students in grades 1 to 12 and claims to be the "Number 1 educational ecosystem in Kazakhstan."

On March 20, 2020, the Kazakhstan Ministry of Education recommended Daryn Online for children's learning during Covid-19 school closures, working with the country's telecommunications providers to zero-rate the website—that is, not charging users for data use when accessing that specific website—to allow students to use it for free.[311] Within days, the website was overwhelmed by 1.5 million new users.[312] In an interview with Forbes Kazakhstan, 27-year old founder Aibek Kuatbaev said, in astonishment, "we could not imagine such an explosive growth," and that this "organic growth took place with the support of the state."[313]

By April 1, 2020, the founder sought to monetize the attention of his newfound user base by posting a "Price List for Advertising" on Daryn Online's home page, offering advertisers the opportunity to advertise to his students.[314] An advertiser could purchase the ability to display an ad banner on the login and registration page—which students had to pass through in order to get to their classes—for 70,000 KZT (US$164) a day, or 420,000 KZT (US$985) for a whole week. Advertisers could also purchase the ability to send out a push notification that would appear on the phones of 800,000 users of Daryn Online's study app for 900,000 KZT (US$2,112).

310 Human Rights Watch identified nine companies with products that appear to have protected their users' data and privacy. These were: Stile Education, Math Kids, learn, Prof Multi, Jitsi, Learning Apps, IServ, Visavid, and Learning Outcomes Smart Q.

311 Ministry of Education and Science of the Republic of Kazakhstan, "Kazakhs will have free access to educational Internet resources" ("Қазақстандықтарға білім беру интернет-ресурстарына тегін кіруге мүмкіндік беріледі"), March 20, 2020, https://www.gov.kz/memleket/entities/edu/press/news/details/49822?lang=kk (accessed July 20, 2021).

312 Anna Reznik, "Kazakhstani startup has provided everyone with free access to online lessons" ("Казахстанский стартап предоставил всем желающим бесплатный доступ к онлайн-урокам"), Forbes Kazakhstan, April 5, 2020, https://forbes.kz//process/kazahstanskiy_startap_predostavil_vsem_besplatnyiy_dostup_k_onlayn-urokam (accessed July 20, 2021).

313 Ibid.

314 Daryn Online, "Price list for advertising on the Daryn.online website" ("Прайс-лист на размещение рекламы на сайте Daryn.online"), https://web.archive.org/web/20210720061302/https:/docs.google.com/spreadsheets/d/1Vz3NkoutAZwtPWqfGb_smdrc_b21kVHS/edit (accessed July 20, 2021).

Human Rights Watch also detected Daryn Online transmitting children's personal data to Google, CloudFlare, Yandex, and Facebook, and found that the website engaged in intrusive surveillance of its students by installing session recorders and key logging.

Daryn Online discloses in their privacy policy that they may use information about a child and what they do in class—including their search history, messages, and comments to teachers, classmates, or written on their homework—"for advertising and sponsorship purposes," and provide "anonymous" data to "third parties, as well as to partners and advertisers."[315] The company also "reserves the right to download advertisements of other organizations on Daryn.online without the User's consent."

Daryn Online did not respond to our request for comment.

Governments Failed to Protect

> Because Spain was in a state of emergency, the Ministry of Education communicated [to teachers] that consent for privacy, or data protection, was no longer required ... Privacy and all that has gone into the background completely, but we have done it because the Ministry has said so.
>
> —Secondary school science teacher, Madrid, Spain[316]

With the exception of a single government—Morocco—all governments reviewed in this report failed to protect children's right to education. Human Rights Watch found that every government endorsed or procured at least one EdTech product that appeared to put at risk or infringed on children's rights. Similarly, the majority of EdTech products endorsed by governments—146 out of 164, or 89 percent—engaged in data practices that appeared to put children's rights at risk or directly infringed on them.

Most EdTech products were marketed as free and provided to governments at no direct financial cost. In the process of endorsing these and promoting their wide adoption by schools, teachers, and students, governments offloaded the true costs of providing education online onto children, who were forced to pay for their learning with their fundamental rights to privacy, access to information, and their freedom of thought.

Most governments failed to take measures to prevent or mitigate children's rights abuses by companies. Few governments appear to have taken child data privacy into consideration in their endorsements of EdTech products. At time of writing, no government reviewed in this report was found to have undertaken a technical privacy evaluation of the EdTech products they recommended after the declaration of the pandemic in March 2020.

315 Daryn Online, "User agreement" ("Қолданушы келісімшарты"), https://web.archive.org/web/20210308190949/https://daryn.online/qoldanushy-kelisimsharty (accessed March 8, 2021).

316 Human Rights Watch interview with secondary school teacher, Madrid, Spain, June 9, 2020.

One government, Australia (New South Wales), conducted assessments for two of its three EdTech recommendations in June 2020 and October 2021.[317] These assessments rely on a self-reported questionnaire completed by an EdTech company, and reviewed by a non-profit company owned by state, territory, and Australian Government education ministers.[318]

Human Rights Watch found that two national education ministries and two state-level ministries—Republic of Korea, Australia (Victoria), Germany (Bavaria), and Poland—provided general data privacy guidance to schools relating to online learning.[319]

Governments that did not carry out children's rights due diligence passed onto children the risks and harms associated with the misuse and exploitation of their personal data, which include security breaches, commercial exploitation, and the use of children's data by governments, law enforcement, and other actors for purposes that are not directly relevant, necessary, or proportionate to children's education or their best interests.[320]

As noted in Chapter 2, for example, Oracle's BlueKai was reported to have exposed billions of people's personal data in one of the largest data security breaches in 2020. Human Rights Watch detected four EdTech products—CBC Kids (Canada), Z-kai (Japan), Notesmaster (Malawi), and EBS (Republic of Korea)—transmitting their students' data to BlueKai through ad trackers and cookies pointing to the domains **bluekai.com** and **bkrtx.com**, both prior to, and after, the reported data breach.

317 Human Rights Watch email correspondence with Sandie Matthews, Chief Information and Data Officer, New South Wales Department of Education, April 14, 2022.

318 Safer Technologies 4 Schools, "About the ST4S Assessment," https://web.archive.org/web/20220313232236/https://st4s.edu.au/general-information/ (accessed May 5, 2022); Education Services Australia, "About Education Services Australia," https://web.archive.org/web/20220423212000/https://www.esa.edu.au/about/about-us (accessed May 5, 2022).

319 Bavarian State Ministry for Education and Culture, "Use online offers in school in a legally compliant manner" ("Online-Angebote rechtssicher in der Schule nutzen"), mebis Infoportal, https://www.mebis.bayern.de/infoportal/service/datenschutz/recht-ds/apps-im-unterricht/ (accessed September 13, 2021); Republic of Korea Ministry of Education, "Please protect teachers and everyone's personal information during remote classes!" ("원격수업 시 선생님 교육활동과 모두의 개인정보를 보호해주세요!"), April 9, 2021, https://www.moe.go.kr/boardCnts/view.do?boardID=340&boardSeq=80261&lev=0&searchType=S&statusYN=W&page=1&s=moe&m=0202&opType= (accessed September 13, 2021); Australia State Government of Victoria, "Online tools for collaboration and learning," July 11, 2021, https://web.archive.org/web/20210423052923/https://www.coronavirus.vic.gov.au/online-tools-collaboration-and-learning (accessed September 13, 2021); Poland Ministry of Education and Science, "Safe personal data during distance learning - the Personal Data Protection Office for schools" ("Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół"), https://zpe.gov.pl/a/dane-osobowe-bezpieczne-podczas-zdalnego-nauczania---poradnik-uodo-dla-szkol/D3VP5T8OL (accessed September 13, 2021). do?boardID=340&boardSeq=80261&lev=0&searchType=S&statusYN=W&page=1&s=moe&m=0202&opType= (accessed September 13, 2021); Australia State Government of Victoria, "Online tools for collaboration and learning," July 11, 2021, https://web.archive.org/web/20210423052923/https://www.coronavirus.vic.gov.au/online-tools-collaboration-and-learning (accessed September 13, 2021); Poland Ministry of Education and Science, "Safe personal data during distance learning - the Personal Data Protection Office for schools" ("Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół"), https://zpe.gov.pl/a/dane-osobowe-bezpieczne-podczas-zdalnego-nauczania---poradnik-uodo-dla-szkol/D3VP5T8OL (accessed September 13, 2021).

320 For further examples, please refer to chapter 2 of this report.

Governments Directly Engage in Rights Violations

Many governments directly built and offered their own EdTech products that violated or put at risk children's rights.

Out of the 42 governments that provided online education to children during the pandemic by directly building and offering their own EdTech products, 39 governments produced products that handled children's personal data in ways that may have put at risk or violated their rights, as described in chapters 2 and 3.

Put another way, out of a total 65 EdTech products built or financed by governments, the majority—56, or 86 percent—were found transmitting children's data to AdTech companies.

56 government-built EdTech products sent children's data to AdTech companies

Government	EdTech Product	Has Privacy Policy?
Argentina	Educ.ar	Yes
Brazil (Minas Gerais)	Estude em Casa	No
Brazil (São Paulo)	Centro de Mídias da Educação de São Paulo	Yes
Burkina Faso	Faso e-Educ@tion	No
Cameroon	Distance Learning	No
Canada (Quebec)	CBC Kids	Yes
Canada (Quebec)	Mathies	No
Canada (Quebec)	PBS Learning	Yes
Chile	Aprendo en Línea	Yes
China	Eduyun	No
Colombia	Aprender Digital	No
Côte d'Ivoire	Mon école à la maison	No
Ecuador	Educa Contigo	No
France	Deutsch für Schulen	Yes
France	English for Schools	Yes
Ghana	Ghana Library App	Yes
Guatemala	Mineduc Digital	Yes
India (Maharashtra, National, Uttar Pradesh)	Diksha	Yes
India (Maharashtra, National, Uttar Pradesh)	e-Pathshala	Yes
India (Maharashtra)	e-Balbharti	Yes
Indonesia	Rumah Belajar	Yes
Iran	Shad	No
Iraq	Newton	No
Kenya	Kenya Education Cloud	No
Malawi	Notesmaster	Yes

Malaysia	DELIMa	No
Mexico	@prende 2.0	Yes
Nepal	Learning Portal	No
Peru	Aprendo en Casa	No
Poland	E-podręczniki	Yes
Republic of Korea	EBS	Yes
Republic of Korea	KERIS edunet	Yes
Republic of Korea	Wedorang	Yes
Russian Federation	Moscow Electronic School	Yes
Russian Federation	My Achievements	Yes
Russian Federation	My School is Online	No
Russian Federation	Digital Lessons	Yes
Russian Federation	Russia Electronic School	Yes
Saudi Arabia	iEN	Yes
South Africa	Department of Basic Education website	Yes
Spain (Andalusia)	eAprendizaje	Yes
Spain (Catalonia)	EDU365.cat	Yes
Spain (Catalonia)	Super3	Yes
Spain (National)	Aprendo en Casa	Yes
Sri Lanka	e-Thaksalawa	No
Sri Lanka	Nenasa	Yes
Taiwan	Education Cloud	Yes
Taiwan	Kaohsiung Daxuetang	Yes
Taiwan	Taipei CooC Cloud	Yes
Thailand	DEEP	Yes
Turkey	Eğitim Bilişim Ağı	No
Turkey	Özelim Eğitimdeyim	Yes
Venezuela	Cada Familia Una Escuela	No
Vietnam	OLM	No
Zambia	e-Learning portal	No
Zambia	Smart Revision	No

Only nine government EdTech products—Educ.ar (Argentina), CBC Kids (Canada), PBS Learning (Canada), Ghana Library App (Ghana), Rumah Belajar (Indonesia), South Africa's Ministry of Education website (South Africa), EBS (Republic of Korea), KERIS edunet (Republic of Korea), and Wedorang (Republic of Korea)—disclosed in their privacy policies that they collect and use students' data for advertising. Of these, four government products—Rumah Belajar, the Education Ministry of South Africa's own website, CBC Kids, and Ghana Library App—explicitly disclosed that they use their students' data for behavioral advertising purposes.

Furthermore, Human Rights Watch identified 22 government EdTech products that failed to offer any privacy policy at all, thus keeping their students in the dark about how their governments were handling their intimate data and their privacy.

In contrast, only eight government-built products were found to protect children's data by not installing any tracking technologies. These were: Juana Manso (Argentina), Biblioteca Digital Escolar (Chile), Jules, MaSpéMaths, and Ma classe à la maison (France), mebis (Germany: Bavaria), NHK for Schools (Japan), and TelmidTICE (Morocco). While few in number, these nine products demonstrate that it is possible for governments to uphold their obligation to protect and promote children's rights by building and offering digital educational services to children that do not compromise their data and their privacy.

Case Study: Zambia

Children with access to connectivity and capable devices, or whose families made sacrifices to ensure their access, relied on EdTech to attend school online during the pandemic. The economic incentives to monetize their captive attention were illustrated in Zambia, a country which legally guarantees free basic education to every child and has committed to provide free and compulsory primary and secondary education, or grades 1 to 12, in its national education plans.[321]

Human Rights Watch found that the Zambian government charged primary and secondary students for the online education it provided during Covid-19 school closures. On April 20, 2020, Zambia's Ministry of General Education launched two websites: the first, e-Learning Portal, offered courses in core subjects for students grades 7 to 12; the second, Smart Revision, provided practice tests to help students in grades 7, 9, and 12 prepare for national examinations.[322]

Both websites required children to pay a monthly subscription fee before they could access learning content. Each course on e-Learning Portal costed ZMW 5 (US$0.26), although students were nudged by the website's design toward subscription bundles that were progressively more expensive at higher grades.[323] For example, the website advertised the option to "Subscribe To All At K35 Only" (at a cost of US$1.84) for students in grades 10-12, even though only three subjects were available to take—Biology, Chemistry, and Mathematics—that would have costed much less to purchase separately.[324] Smart Revision featured similarly tiered pricing, and charged a monthly fee of ZMW 10 (US$0.53) for students in grade 7, ZMW 20 (US$1.05) for grade 9 students, and ZMW 30 (US$1.58) for students in grade 12.[325]

321 The Education Act, Act 23 of 2011, Part IV, art. 15; Republic of Zambia, Ministry of Education, "Education Sector National Implementation Framework III 2011-2015,"June 2010, https://planipolis.iiep.unesco.org/sites/default/files/ressources/zambia_education_sector_nif_iii_2011_2015_final_draft.pdf (accessed May 16, 2022), p. xvi; Government of Zambia, Free Primary Education Policy of 2002; Government of Zambia, Fifth to Seventh Periodic Reports to the Committee on the Rights of the Child, CRC/C/ZMB/5-7, November 11, 2021, Section H, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fZMB%2f5-7&Lang=en (accessed August 23, 2021), para. 149,

322 Zamtel, "Zamtel Launches E-Learning and Smart Revision Portal," https://web.archive.org/web/20210823192902/https://www.zamtel.zm/news_elearning.html (accessed August 23, 2021); "Zamtel, ECZ and Ministry of General Education launch e-Learning and Smart Revision portals," *Lusaka Times*, April 21, 2020, https://www.lusakatimes.com/2020/04/21/zamtel-ecz-and-ministry-of-general-education-launch-e-learning-and-smart-revision-portals/ (accessed August 23, 2021).

323 Government of Zambia, Ministry of General Education, E-Learning Portal, "Subscription," https://web.archive.org/web/20210823165611/https://elearning.co.zm/subscription/ (accessed August 23, 2021); see also: Government of Zambia, Ministry of General Education, E-Learning Portal, "E-Learning," https://web.archive.org/web/20210823163825/https://elearning.co.zm/e-learning/ (accessed August 23, 2021).

324 Ministry of General Education, E-Learning Portal, "Grade 10-12 All Subjects," https://web.archive.org/web/20210823205605/https://elearning.co.zm/grade-10-12-all-subjects/ (accessed August 23, 2021).

325 Examinations Council of Zambia, Zamtel, Smart Revision, "Grade," https://web.archive.org/web/20210823192047/https://www.smartrevision.co.zm/grade.php (accessed August 23, 2021); see also: "Terms and Conditions," https://web.archive.org/web/20210823192347/https://www.smartrevision.co.zm/termsandconditions.php (accessed August 23, 2021).

These fees constituted a direct cost and a financial barrier to education, in addition to the high costs of internet access and devices that students and their families had to pay for before they could even access either of the government's websites.[326] Access to the internet in Zambia is prohibitively expensive for many, especially for the poorest children and those living in rural areas. According to the Inclusive Internet Index report, Zambia ranks 98 out of 120 countries surveyed in the cost of internet access relative to income.[327] In 2015, 57.5 percent of Zambia's population lived below the international poverty line of US$1.90 per day; poverty is estimated to have increased with widespread job losses and rising prices during the pandemic, making the internet even less affordable for most children and their families.[328]

Human Rights Watch also detected e-Learning Portal transmitting its students' personal data to PushEngage, a company offering push notification services "so you can unlock maximum revenue from each visitor," and Tawk.to, a live chat service, even though the latter function was neither visible nor available for use on e-Learning Portal's website.[329] Human Rights Watch detected Smart Revision sending students' personal data to Facebook.

For students relying on these websites to learn core content and prepare for high-stakes national examinations during Covid-19 school closures, submitting to these data practices was an indirect cost levied on them in exchange for their education.

The Zambian government, e-Learning Portal, PushEngage, and Smart Revision did not respond to a request for comment. Tawk.to and Facebook did not acknowledge Human Rights Watch's finding that they were receiving data from either of these websites, or respond to questions about it.

No Choice

As noted in Chapter 3, this data collection and surveillance took place in virtual classrooms and educational settings where children could not reasonably object to such surveillance. Most government-built EdTech platforms did not allow their users to decline to be tracked; most of this surveillance happened secretly, without the child's knowledge or consent. In such cases, it was impossible for children to opt out of such surveillance and data exploitation without opting out of school and giving up on formal learning altogether during the pandemic.

Some governments made it compulsory for students and teachers to use government-built EdTech platforms, not only subjecting them to the data practices and privacy protections—or lack thereof—of those products, but also making it impossible for children to protect themselves by opting for alternative means to access their right to education.

Teachers in Iran told Human Rights Watch that the government compelled those in public schools to use Shad, an app built by Iran's Education Ministry for online learning during Covid-19.[330] One teacher said: "The principal called and said that if I do not install the Shad app, I would be recorded as absent. The authorities do not accept teaching in Telegram and WhatsApp.... Students have also been told that if you are not in this app, your score will not be approved and will not be sent to the [school]."[331] In October 2021, the Iranian government reported more than 18 million active users of Shad.[332]

326 Both websites were launched in partnership with Zamtel, the state-owned telecommunications provider and one of the three mobile internet providers in the country. While Zamtel announced that it would zero-rate both websites—that is, to provide free access to these websites by not charging users for data— Human Rights Watch notes that children would realistically first need internet access to even be aware of the government's websites.

327 The Economist Intelligence Unit, "The Inclusive Internet Index, 2021" https://theinclusiveinternet.eiu.com/explore/countries/ZM/performance/indicators/affordability (accessed August 23, 2021).

328 World Bank, "Poverty and Equity Brief: Zambia," April 2020, https://databank.worldbank.org/data/download/poverty/33EF03BB-9722-4AE2-ABC7-AA2972D68AFE/Global_POVEQ_ZMB.pdf (accessed August 23, 2021).

329 PushEngage, "PushEngage," https://web.archive.org/web/20210915214533/https://www.pushengage.com/ (accessed September 15, 2021).

330 Salman Parviz, "Schools Set to Open Sept. 5 Amid Pandemic," *Tehran Times*, September 5, 2020, https://www.tehrantimes.com/news/452046/Schools-set-to-open-Sept-5-amid-pandemic (accessed November 16, 2020); Alijani Ershad, "In Iran, poverty and lack of internet make distance learning impossible," France24, April 21, 2020, https://observers.france24.com/en/20200421-iran-internet-covid19-distance-learning-poverty (accessed November 16, 2020).

331 Human Rights Watch interview with teacher, Marivan, Iran, May 4, 2020.

332 Government of Iran, Ministry of Education, "Shad," https://web.archive.org/web/20211028212342/http://www.shad.ir/ (accessed October 28, 2021).

Technical analysis of Shad's code by Human Rights Watch found that the app can collect children's precise location data, the time of their current location, the child's last known location, their Wi-Fi SSID, IP address, the child's contacts, and any saved photos of their contacts.

Iran does not have a data protection law. A Personal Data Protection and Safeguarding Draft Act ("Draft Act") was first proposed on July 26, 2018, and is still pending review from the Islamic Parliament of Iran as of September 2021; the Draft Act does not contain specific protections for children.[333]

In Turkey, one mother of a 9-year-old child, Rodin, told Human Rights Watch: "Rodin's teacher forced all these 8-year-old kids to use Facebook. He made Rodin, who was 8 at the time, open a Facebook account, and told him to upload his homework there. Now, the teacher is forcing the kids to use Facebook when they're taking tests."[334] Facebook's terms of service prohibit children under 13 years old from using its services.[335]

She continued, "The teacher also asked me to download BiP [a government-mandated messaging app for government and school use during the pandemic] to communicate with him. I'd heard that the app was not secure in terms of data privacy, so I said no. The teacher said, 'Well, then you can't communicate with me.' I didn't want to download the app, so I told him, 'I don't have space on my phone.' The teacher said, 'Well, you can't communicate with me,' and blocked us all on WhatsApp to prevent all parents from contacting him on secure apps. So, I haven't been able to talk to him since."[336]

As noted in Chapter 2, the Indian government offered Diksha, an app that claimed to deliver education to over 10 million students in the early days of the pandemic. To drive further adoption, some state-level education ministries set quotas for government teachers to compel a minimum number of students to download the app.[337]

Human Rights Watch found that Diksha collects children's precise location data, including the time of their current location and their last known location. Human Rights Watch also observed Diksha collecting and transmitting children's AAID to Google, which demonstrates that Diksha shares children's personal data with Google for advertising purposes.

In these countries, children could not give valid, meaningful consent for the processing of their data by government-mandated EdTech platforms—even if they had been asked—because they could not refuse to use them freely without detrimental effect, and there were no alternative means to access their education.

333 Government of Iran Ministry of Communications and Information Technology, "Draft Protection of Personal Data Law" ("از داده‌های شخصی صیانت و حفاظت"), https://web.archive.org/web/20210611152356/https://www.ict.gov.ir/fa/newsagency/21691/%D9%84%D8%A7%DB%8C%D8%AD%D9%87%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%88%D8%AD%D9%81%D8%A7%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D9%87%D8%A7%DB%8C%D8%B4%D8%AE%D8%B5%DB%8C-%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C%D8%B4%D8%AF (accessed September 20, 2021); OneTrust DataGuidance, "Iran," https://www.dataguidance.com/jurisdiction/iran (accessed September 20, 2021.

334 Human Rights Watch interview with mother, Istanbul, Turkey, June 11, 2021.

335 Facebook, "Terms of Service," https://www.facebook.com/legal/terms (accessed September 15, 2021), 3(1).

336 Human Rights Watch interview with mother, Istanbul, Turkey, June 11, 2021.

337 Ishita Bhatia, "Remote learning: UP sets target, tells each govt teacher to convince 10 students to download Diksha app," Times of India, November 18, 2020, https://timesofindia.indiatimes.com/city/meerut/remote-learning-up-sets-target-tells-each-govt-teacher-to-convince-10-students-to-download-diksha-app/articleshow/79268507.cms (accessed August 24, 2021).

Acknowledgments

This report was researched and written by Hye Jung Han, researcher and advocate in the children's rights division at Human Rights Watch, who also conducted technical static analysis of all EdTech apps, technical analysis of EdTech websites, and data analysis of all EdTech products.

Technical analysis of EdTech websites was also conducted by Gabi Ivens, head of open source research at Human Rights Watch, and guided by Surya Mattu, Senior Data Engineer and Investigative Data Journalist of The Markup. We are particularly grateful to Surya Mattu for his work in building Blacklight, the real-time website privacy inspector built for The Markup, and for his generous assistance and invaluable insights in adapting the tool for Human Rights Watch's website analysis.

Additional technical analysis—both static and dynamic—of eight EdTech apps was conducted by Esther Onfroy, founder of Defensive Lab Agency, who also conducted additional dynamic analysis and ran the data experiments with four children located in Indonesia, India, South Africa, and Turkey. We are extremely grateful to Esther Onfroy for her work, as well as for her generous technical advice and expertise.

Additional interviews were conducted by Marlene Auer, former associate, Europe and Central Asia (ECA); Martha Bernild, associate, Development and Global initiatives; Hanna Darroll, former senior associate, Development and Global Initiatives; Tayla Hall, senior coordinator, Development and Global Initiatives; Anjelica Jarrett, former coordinator, LGBT rights; Aya Majzoub, researcher, Middle East and North Africa (MENA); Devin Milroy, former associate, Global IT; Elin Martínez, senior researcher, children's rights; Seung Kyung Noh, former senior associate, Operations; Catherine Pilishvili, senior coordinator, ECA; Marina Riera Rodoreda, former coordinator, International Justice; Anna Salami, officer, Development and Global initiatives; Kristen Scott, senior associate, Development and Global initiatives; Delphine Starr, former senior coordinator, children's rights; Svetlana Stepanova, senior manager, Development and Global initiatives; Behrouz Tehrani, consultant, MENA; Agnes Tkotz, associate director, Development and Global initiatives; Nicole Tooby, officer, Asia; Frances Underhill, senior manager, Film Festival; and Tenzin Wangmo, officer, General Counsel.

This report was edited by Bede Sheppard, children's rights deputy director at Human Rights Watch. Maria McFarland Sánchez-Moreno, senior legal advisor, and Tom Porteous, deputy program director, provided legal and program reviews. Expert reviews were provided by: Ilaria Allegrozzi, senior researcher, Africa; Jayshree Bajoria, senior researcher, Asia; Julia Bleckner, Asia researcher and health editor; Deborah Brown, senior researcher and advocate, technology and human rights; Eva Cossé, researcher, ECA; Farida Deif, Canada director; Corinne Dufka, associate director, Africa; Anietie Ewang, researcher, Africa; Elvire Fondacci, coordinator, France; Lydia Gall, senior researcher, ECA; Abir Ghattas, director, Information Security; Andreas Harsono, senior researcher, Asia; Saroop Ijaz, senior researcher, Asia; Paula Ini, senior research assistant, Americas; Gabi Ivens, head of open source research; Teppei Kasai, officer, Asia; Chloe King, researcher, MENA; Anastasiia Kruope, assistant researcher, ECA; Linda Lakhdhir, legal advisor, Asia; Elin Martínez, senior researcher, children's rights; Tyler Mattiace, researcher, Americas; Sophie McNeill, researcher, Asia; Santiago Menna, research assistant, Americas; César Muñoz , senior researcher, Americas; Otsieno Namwaya, senior researcher, Africa; Juan Pappier, senior researcher, Americas; Laura Pitter, deputy director, United States; Sunai Phasuk, senior researcher, Asia; Martina Rapido Ragozzino, senior research assistant, Americas; Kartik Raj, researcher, ECA; Mihra Rittmann, senior researcher, ECA; Tara Sepehri Far, senior researcher, MENA; Mary Smith, researcher, Asia; Judith Sutherland, associate director, ECA; Tamara Taraciuk Broner, acting director, Americas; Nathalye Cotrino Villarreal, senior research assistant, Americas; Maya Wang, senior researcher, Asia; Belkis Wille, senior researcher, crisis and conflict; Lina Yoon, senior researcher, Asia; and Hiba Zayadin, senior researcher, MENA.

Acknowledgments

Additional colleagues provided expert review for this report but are not named here for security reasons.

We are grateful to Esther Onfroy and Surya Mattu for providing external expert technical review.

External legal review was provided by Elizabeth Wang, founder of Elizabeth Wang Law Offices.

Sakae Ishikawa, senior video editor at Human Rights Watch, Liliana Patterson, senior editor, and Christina Curtis, multimedia deputy director, produced and edited one of the accompanying videos. Priya Sanghvi, content and production strategist, managed the production of a second accompanying video, which was produced and edited by by Alejandro Norman, Patrick Scerri, Andrea Devia-Nuño, Erik Righetti, Hanna Lau-Walker, and Min Liu at Hero Studios.

Production assistance was provided by Katherine La Puente, associate, children's rights; Travis Carr, senior publications coordinator; and Fitzroy Hepkins, senior administrative manager. Content strategy, branding, and design was provided by Deroy Peraza, Izabella Stern, Lauren Jones, Pauline Shin, and Rima Desai of Hyperakt; and illustration was provided by Andrea Devia-Nuño at Hero Studios. Design direction and operational support was provided by Grace Choi, director of publications and information design; Les Lim, developer; and Christina Rutherford; senior digital manager.

The campaign supporting this project was led by Amanda Alampi, deputy director, Campaigns and Public Engagement; Ziva Luddy Juneja, acting digital campaigner; Bronte Price, digital engagement strategist; Nailah Ali, senior graphic designer, public engagement; and supported by Andrea Zita, associate; and Naimah Hakim, senior coordinator. Emma Daly, head of the Collaboratory, provided support and guidance.

We thank the four children and their parents who were willing to test out specific EdTech apps recommended by their government in order to verify our findings, and shared their stories with us.

Human Rights Watch thanks the Novo Nordisk Foundation for their support of this project.

“How Dare They Peep into My Private Life?”

Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic

“*How Dare They Peep into My Private Life?’: Children’s Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic*,” is a global investigation of the education technology (EdTech) endorsed by 49 governments for children’s education during the pandemic. Based on technical and policy analysis of 164 EdTech products, Human Rights Watch finds that the majority of these online learning platforms put at risk or infringed upon children’s privacy and other rights, for purposes unrelated to their education.

These products monitored children, harvesting personal data such as who they are, where they are, what they do in the classroom, who their family and friends are, and what kind of device their families could afford for them to use. Children, parents, and teachers were largely kept in the dark about these data surveillance practices.

The report finds that governments failed to protect children’s right to education. By endorsing and enabling the wide adoption of EdTech products without adequate safeguards or oversight, governments offloaded the true costs of providing online education onto children, who were unknowingly forced to pay for their learning with their rights to privacy and access to information, and potentially their freedom of thought.

Children’s reliance on digital services that enable their education will likely continue long after the end of the pandemic. Governments should adopt modern child data protection laws to protect children online. Companies should immediately stop collecting, processing, and sharing children’s data in ways that risk or infringe on their rights.